VIRGINIA:

IN THE CIRCUIT COURT OF FAIRFAX COUNTY

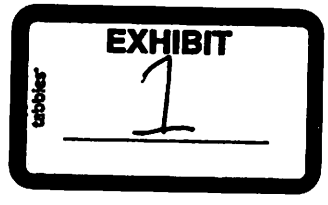
VERISIGN, INC., Plaintiff, v. CENTRALNIC LIMITED, XYZ.COM LLC Serve: Paracorp Incorporated, Reg. Agt. 318 N. Carson Street, Suite 208 Carson City, NV 89701 -and- DANIEL NEGARI, 205 South Camden Drive Beverly Hills, CA 90212 Defendants.	)	Civil Action No. CL 2015-3519

FIRST AMENDED COMPLAINT

COMES NOW the plaintiff, VeriSign, Inc. ("Verisign"), by counsel, and for its first amended complaint states the following:

Parties

1. Verisign is a corporation organized and existing under the laws of the State of Delaware, having its principal place of business in the Commonwealth of Virginia.



2. Defendant CentralNic Limited ("CentralNic") is a corporation organized and existing under the laws of the United Kingdom, having its principal place of business in London, England.

3. Defendant XYZ.COM LLC ("XYZ") is a limited liability company organized and existing under the laws of the State of Nevada, having its principal place of business in the State of Nevada.

4. Defendant Daniel Negari is a natural person who, upon information and belief, is a resident of the State of California. Upon information and belief, Negari owns and/or controls XYZ.

Jurisdiction and Venue

5. This Court has subject matter jurisdiction over this action pursuant to Virginia Code § 17.1-513.

6. CentralNic, XYZ and Negari are subject to personal jurisdiction in this Court pursuant to Virginia Code § 8.01-328.1(3 & 4) in that, as set forth herein, CentralNic, XYZ and Negari have caused tortious injury by acts in this Commonwealth; and have caused tortious injury in this Commonwealth by acts and omissions outside this Commonwealth and regularly do or solicit business, or engage in other persistent course of conduct in this Commonwealth. In addition, as set forth herein, CentralNic, XYZ and Negari have tortiously interfered with contracts which provide for jurisdiction and venue to lie in this Court.

7. Venue is appropriate in this Court pursuant to Virginia Code § 8.01-262. In addition, CentralNic, XYZ and Negari, by tortiously interfering with the KBE MSA and Symantec MSA (as defined below), consented to venue in this Court.

Facts

The New gTLD Program

8. In 2008, the Internet Corporation for Assigned Names and Numbers ("ICANN") approved a program for the launch of new generic top level domains ("gTLDs") in the Internet's addressing system. A top-level domain ("TLD") is, in simple terms, the letters to the right of the "dot" in a domain name, e.g., <.com> or <.org>. Unlike a country-code TLD ("ccTLD"), which generally is assigned to a country, sovereign state or dependent territory (e.g., <.uk>, <.cn>), a gTLD is one associated with a "generic" term such as <.com> or <.org>.

9. As part of ICANN's new gTLD program, persons and entities were permitted to apply, for a fee, for the rights to serve as the exclusive registry for proposed gTLDs. Some of these applicants were brand owners, seeking a gTLD for their brands (e.g., <.bmw>, <.suzuki>). Others applied for gTLDs that might have a broad appeal (e.g., <.web>), while others applied for gTLDs that might appeal to groups with special interests (e.g., <.attorney>, <.tires>).

10. Each applicant for a gTLD was required to demonstrate to ICANN that it was able to provide technically competent registry services for its proposed gTLD.

11. Verisign is, and has since 2000 been, the registry operator for the largest gTLD, <.com>, together with a number of other TLDs. For some of these TLDs such

as <.com> and <.net>, Verisign has direct agreements with ICANN to operate the registries. In other cases, Verisign operates the registries under agreements with the parties authorized to operate the TLD (e.g., <.gov>, <.tv>).

12. As a result of Verisign's expertise as a registry operator, it has entered into agreements with applicants for some of the new gTLDs to provide certain back-end registry services for the applicants' new gTLDs.

The KBE Agreements

13. On April 12, 2012, Key Brand Entertainment, Inc. ("Key Brand") entered into a "Verisign Master Services Agreement" ("KBE MSA") with Verisign, which set forth various terms relating to Verisign's general provision of services to Key Brand and its Affiliates (as that term is defined in the MSA), and contemplated service orders between Verisign and Key Brand and its Affiliates. A copy of the KBE MSA was filed under seal herein on May 13, 2015.

14. On April 12, 2012, KBE GTLD Holding, Inc. ("KBE Holding") (together with Key Brand, "KBE") entered into a "Verisign New gTLD Services SO" Service Order (the "KBE Service Order") with Verisign which, in conjunction with the KBE MSA, sets forth various terms relating to Verisign's provision of "New gTLD Services" (as defined in the KBE Service Order) with respect to KBE's applied-for gTLDs. A copy of the KBE Service Order was filed under seal herein on May 13, 2015.

15. Under the terms of the KBE Service Order, Key Brand agreed to "guarantee[] the performance and payment obligations of KBE [] under the [KBE] MSA, this SO, and each order form hereunder."

16. Pursuant to, and attached to, the KBE Service Order, KBE executed and delivered order forms with respect the gTLDs <.broadway>, <.bway>, <.theater>, and <.theatre>.

17. On June 13, 2012, KBE applied to ICANN to be the registry operator for all four of these applied-for gTLDs.

18. KBE subsequently withdrew its applications for the <.broadway>, <.bway>, and <.theater> gTLDs. As a result, the parties' obligations under the MSA and the Service Order with respect thereto were terminated.

19. Pursuant to the KBE MSA and the KBE Service Order, KBE purchased Verisign's New gTLD Services (as defined in the KBE MSA) for the gTLD <.theatre> (hereinafter, the "KBE gTLD").

20. The KBE Service Order also incorporates by reference the Service Guide for New gTLD Services (the "Service Guide"), which is attached to the KBE Service Order.

21. The Service Guide provides that KBE "shall not change any information, data or document provided by Verisign or fail to use the responses provided by Verisign for the questions regarding Technical and Operational Capability of the TLD (as described herein) [in its applications with ICANN] without Verisign's prior written consent."

The KBE Applications

22. On or about June 13, 2012, KBE submitted its initial application for the KBE gTLD to ICANN.[1] A copy of this application is attached hereto, incorporated herein, and marked as *Exhibit 1*.

23. As required by the KBE Service Order, KBE's initial application to ICANN for the KBE gTLD identified Verisign as the exclusive provider of back-end registry services for the KBE gTLD, and included Verisign's specifications and responses regarding technical and operational capability of the KBE gTLD that Verisign previously provided to KBE pursuant to the terms of the KBE Service Order.

24. KBE's application to ICANN for the KBE gTLD passed ICANN's initial evaluation process on June 7, 2013.

25. On or about October 10, 2014, KBE submitted to ICANN a request to change its application for the KBE gTLD. A copy of this amendment is attached hereto, incorporated herein, and marked as *Exhibit 2*.

26. In its change request attached hereto as *Exhibit 2*, KBE removed the reference to Verisign as the provider of back-end registry services, and deleted Verisign's specifications and responses regarding technical and operational capability of the KBE gTLD.

27. In its change request attached hereto as *Exhibit 2*, KBE identified CentralNic as the provider of back-end registry services, and substituted CentralNic's

[1] This application states that the applicant is "Key GTLD Holding, Inc." This appears to be a typographical error.

specifications and responses regarding technical and operational capability of the KBE gTLD where Verisign's previously had appeared.

28. ICANN approved KBE's change request on December 19, 2014.

The Symantec Agreements

29. Effective as of August 9, 20101, Symantec Corporation ("Symantec") entered into a "Verisign Master Services Agreement" ("Original Symantec MSA") with Verisign, which set forth various terms relating to Verisign's general provision of services to Symantec and its Affiliates (as that term is defined in the Original Symantec MSA), and contemplated service orders between Verisign and Symantec and its Affiliates. The Original Symantec MSA was amended by "Amendment to Verisign Master Services Agreement" effective as of April 2, 2012 (the "Amendment"). Copies of the Original Symantec MSA and the Amendment are being filed under seal at the time of the filing of this First Amended Complaint. Together, the Original Symantec MSA and the Amendment will hereinafter be referred to as the "Symantec MSA".

30. Effective as of April 2, 2012, Symantec also entered into a "Verisign New gTLD Services SO" Service Order (the "Symantec Service Order") with Verisign which, in conjunction with the Symantec MSA, sets forth various terms relating to Verisign's provision of "New gTLD Services" (as defined in the Symantec Service Order) with respect to Symantec's applied-for gTLDs. A copy of the Symantec Service Order is being filed under seal at the time of the filing of this First Amended Complaint.

31. Pursuant to, and attached to, the Symantec Service Order, Symantec executed and delivered order forms with respect the gTLDs <.protection> and <.security> (the "Symantec gTLDs").

32. On June 13, 2012, Symantec applied to ICANN to be the registry operator for the Symantec gTLDs.

33. Pursuant to the Symantec MSA and the Symantec Service Order, Symantec purchased Verisign's New gTLD Services (as defined in the Symantec MSA) for the Symantec GTLDs.

34. The Symantec Service Order also incorporates by reference the Service Guide, which is attached to the Symantec Service Order.

The Symantec Applications

35. On or about June 13, 2012, Symantec submitted its initial applications for the Symantec gTLDs to ICANN. A copy of the application for <.protection> is attached hereto, incorporated herein, and marked as *Exhibit 3*. A copy of the application for <.security> is attached hereto, incorporated herein, and marked as *Exhibit 4*.

36. As required by the Symantec Service Order, Symantec's initial applications to ICANN for the Symantec gTLDs identified Verisign as the exclusive provider of back-end registry services for the Symantec gTLDs, and included Verisign's specifications and responses regarding technical and operational capability of the Symantec gTLDs that Verisign previously provided to Symantec pursuant to the terms of the Symantec Service Order.

37. In or around September 2014, Symantec sought to terminate the Symantec MSA and the Symantec Service Order, without any permissible basis under the Symantec MSA or the Symantec Service Order.

38. After terminating the Symantec MSA and the Symantec Service Order, on or about February 9, 2015, Symantec submitted to ICANN requests to change its applications for the Symantec gTLDs. A copy of the amendment with respect to <.protection> is attached hereto, incorporated herein, and marked as *Exhibit 5*. A copy of the amendment with respect to <.security> is attached hereto, incorporated herein, and marked as *Exhibit 6*.

39. In its change requests attached hereto as *Exhibits 5 and 6*, Symantec removed the reference to Verisign as the provider of back-end registry services, and deleted Verisign's specifications and responses regarding technical and operational capability of the Symantec gTLDs.

40. In its change requests attached hereto as *Exhibits 5 and 6*, Symantec identified CentralNic as the provider of back-end registry services, and substituted CentralNic's specifications and responses regarding technical and operational capability of the Symantec gTLDs where Verisign's previously had appeared.

41. ICANN approved Symantec's change requests on April 3, 2015.

Why KBE and Symantec Deleted Verisign From its Application

42. KBE decided to sell and transfer its application for the KBE gTLD to XYZ.

43. Symantec decided to sell and transfer its application for the Symantec gTLDs to XYZ.

44. XYZ and Negari demanded, as conditions to XYZ's agreement to purchase the KBE gTLD application, that KBE breach the KBE MSA and the KBE Service Order. A copy of a Purchase Agreement between XYZ and KBE Holding, wherein XYZ required that KBE Holding breach the KBE MSA and KBE Service Order, is being filed under seal at the time of the filing of this First Amended Complaint.

45. Upon information and belief, XYZ and Negari demanded, as conditions to XYZ's agreement to purchase the Symantec gTLDs applications, that Symantec wrongfully terminate and breach the Symantec MSA and the Symantec Service Order.

46. XYZ, at the insistence of Negari, has entered into an agreement with CentralNic to provide back-end registry services for the KBE gTLD, and to remove Verisign as the provider of back-end registry services for the KBE gTLD.

47. XYZ, at the insistence of Negari, has entered into an agreement with CentralNic to provide back-end registry services for the Symantec gTLDs, and to remove Verisign as the provider of back-end registry services for the Symantec gTLDs.

Count 1
Tortious Interference with Contract – KBE gTLD

48. The allegations in paragraphs 1 through 47 are incorporated herein as if fully set forth.

49. The KBE MSA and KBE Service Order were and are valid contracts between Verisign and Key Brand and KBE Holdings.

50. CentralNic, XYZ and Negari, at all times relevant hereto, knew of the existence of the KBE MSA and KBE Service Order, and that Key Brand and KBE Holdings were and are obligated to use Verisign as the exclusive provider of back-end registry services for the KBE gTLD.

51. CentralNic, XYZ and Negari intentionally, willfully and knowingly caused and induced Key Brand and KBE Holdings to breach the KBE MSA and KBE Service Order by replacing Verisign with CentralNic as the provider of back-end registry services in the applications for the KBE gTLD.

52. As a result of CentralNic's, XYZ's and Negari's tortious interference with Verisign's contracts with KBE and Key Brands, Verisign has and will continue to suffer damages.

WHEREFORE, Verisign requests:

a. That judgment be entered in its favor, and against CentralNic, XYZ and Negari, jointly and severally, in the principal sum of $175,000, plus prejudgment and post judgment interest, plus costs; and

b. That the Court afford it such other and further relief as may be appropriate.

Count 2
Tortious Interference with Contract – Symantec gTLDs

53. The allegations in paragraphs 1 through 47 are incorporated herein as if fully set forth.

54. The Symantec MSA and Symantec Service Order were valid contracts between Verisign and Symantec.

55. CentralNic, XYZ and Negari, at all times relevant hereto, knew of the existence of the Symantec MSA and Symantec Service Order, and that Symantec was obligated to use Verisign as the exclusive provider of back-end registry services for the Symantec gTLDs.

56. CentralNic, XYZ and Negari intentionally, willfully and knowingly caused and induced Symantec to breach the Symantec MSA and Symantec Service Order by replacing Verisign with CentralNic as the provider of back-end registry services in the applications for the Symantec gTLDs.

57. As a result of CentralNic's, XYZ's and Negari's tortious interference with Verisign's contracts with Symantec, Verisign has and will continue to suffer damages.

WHEREFORE, Verisign requests:

a. That judgment be entered in its favor, and against CentralNic, XYZ and Negari, jointly and severally, in the principal sum of $332,500, plus prejudgment and post judgment interest, plus costs; and

b. That the Court afford it such other and further relief as may be appropriate.

Count 3
Business Conspiracy (Va. Code §§ 18.2-499, -500) – All Defendants

58. The allegations in paragraphs 1 through 57 are incorporated herein as if fully set forth.

59. XYZ, Negari and CentralNic combined, associated, agreed, mutually undertook and concerted together for the purpose of willfully and maliciously injuring Verisign in its business, by seeking to circumvent Key Brands', KBE Holdings' and Symantec's contractual requirements; by undermining Verisign's contractual right to be the exclusive provider of back-end registry services for the KBE gTLD and the Symantec gTLDs; and by breaching and inducing breaches of the KBE MSA, KBE Service Order, Symantec MSA, and Symantec Service Order.

60. As a result of XYZ's, Negari's and CentralNic's conspiracy as aforesaid and their tortious interference with Verisign's contracts with KBE Holdings, Key Brands and Symantec, Verisign has and will continue to suffer damages.

61. Pursuant to Va. Code § 18.2-500, Verisign is entitled to recover treble damages, costs, attorneys' fees, and is also entitled to injunctive relief.

WHEREFORE, Verisign requests:

a. That judgment be entered in its favor, and against CentralNic, XYZ and Negari, jointly and severally, in the principal sum of $1,552,500, plus prejudgment and post judgment interest, plus costs, plus its attorneys' fees;

b. That CentralNic, XYZ and Negari be enjoined from participating in any combination, association, agreement, mutual undertaking or concerted action injuring Verisign in its business;

c. That CentralNic be preliminarily and permanently enjoined from providing back-end registry services in the application for the KBE gTLD and the Symantec gTLDs; and

d. That the Court afford it such other and further relief as may be appropriate.

Demand for Attorneys' Fees

Pursuant to Rule 3:25, Verisign demands an award of its attorneys' fees, pursuant to Virginia Code § 18.2-500.

VERISIGN, INC.
By Counsel

HYLAND LAW PLLC
1818 Library Street, Suite 500
Reston, Virginia 20190
(703) 956-3566
Facsimile (703) 935-0349
Email thyland@hylandpllc.com
edwyer@hylandpllc.com

By: _____
Timothy B. Hyland (VSB No. 31163)
Elizabeth A. Dwyer (VSB No. 87486)
Counsel for Verisign

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that true copies of this First Amended Complaint were hand delivered this 15th day of July, 2015, to:

Kevin B. Bedell, Esquire
GREENBERG TRAURIG, LLP
1750 Tysons Boulevard, Suite 1200
McLean, VA 22102

Joanna L. Faust, Esquire
CAMERON/MCEVOY PLLC
4100 Monument Corner Drive, Suite 420
Fairfax, VA 22030

_____
Timothy B. Hyland

SPS

COMMONWEALTH OF VIRGINIA
CIRCUIT COURT OF FAIRFAX COUNTY
4110 CHAIN BRIDGE ROAD
FAIRFAX, VIRGINIA 22030
703-691-7320
(Press 3, Press 1)

VeriSign Inc vs. Key Brand Entertainment Inc et al.

CL-2015-0003519

TO: **Key Brand Entertainment Inc.**
Serve: Corporation Service Company
2711 Centerville Road Suite 400
Wilmington DE 19808

SUMMONS – CIVIL ACTION

The party upon whom this summons and the attached complaint are served is hereby notified that unless within 21 days after such service, response is made by filing in the Clerk's office of this Court a pleading in writing, in proper legal form, the allegations and charges may be taken as admitted and the court may enter an order, judgment or decree against such party either by default or after hearing evidence.

APPEARANCE IN PERSON IS NOT REQUIRED BY THIS SUMMONS.

Done in the name of the Commonwealth of Virginia, on March 18, 2015.

JOHN T. FREY, CLERK
By: Daisy M. Eskrez
Deputy Clerk

Plaintiff's Attorney: Timothy B. Hyland

VIRGINIA:

IN THE CIRCUIT COURT OF FAIRFAX COUNTY

VERISIGN, INC.,

Plaintiff,

v.

Civil Action No. 2015-03519

KEY BRAND ENTERTAINMENT, INC.,
Serve: Corporation Service Company
2711 Centerville Road, Suite 400
Wilmington, DE 19808

KBE GTLD HOLDING, INC.,
Serve: Corporation Service Company
2711 Centerville Road, Suite 400
Wilmington, DE 19808

CENTRALNIC LIMITED,
35 - 39 Moorgate, 6th Floor
London EC2R 6AR
United Kingdom

MATTER STRATEGIC ADVISORS, LLC,
Serve: Matthew Russotti, Agent
420 Lexington Ave., Suite 2750
New York, NY 10170

-and-

ENTITY DOE,

Defendants.

COMPLAINT

COMES NOW the plaintiff, VeriSign, Inc. ("Verisign"), by counsel, and for its complaint states the following:

Parties

1. Verisign is a corporation organized and existing under the laws of the State of Delaware, having its principal place of business in the Commonwealth of Virginia.

2. Defendant Key Brand Entertainment, Inc. ("Key Brand") is a corporation organized and existing under the laws of the State of Delaware, having its principal place of business in the State of New York.

3. Defendant KBE GLTD Holding, Inc. ("KBE Holding") is a corporation organized and existing under the laws of the State of Delaware, having its principal place of business in the State of New York.

4. Defendant CentralNic Limited ("CentralNic") is a corporation organized and existing under the laws of the United Kingdom, having its principal place of business in London, England.

5. Defendant Matter Strategic Advisors, LLC ("Matter Strategic") is a limited liability company organized and existing under the laws of the State of New York, having its principal place of business in the State of New York. Upon information and belief, Matter Strategic is the successor in interest to MJRC Group, LLC ("MJRC")

6. Defendant Entity Doe ("Doe") is an entity whose identity is unknown at this time.

Jurisdiction and Venue

7. This Court has subject matter jurisdiction over this action pursuant to Virginia Code § 17.1-513.

8. Key Brand and KBE Holding (hereinafter together, "KBE") are subject to personal jurisdiction in this Court pursuant to Virginia Code § 8.01-328.1(1, 3 and 4) in that, as set forth herein, KBE has transacted business in the Commonwealth of Virginia; has caused tortious injury by acts in this Commonwealth; and has caused tortious injury in this Commonwealth by acts and omissions outside this Commonwealth and regularly does or solicits business, or engages in any other persistent course of conduct. In addition, KBE contractually consented in the MSA (as defined below) to the jurisdiction of this Court.

9. CentralNic, Matter Strategic and Doe are subject to personal jurisdiction in this Court pursuant to Virginia Code § 8.01-328.1(3 & 4) in that, as set forth herein, CentralNic, Matter Strategic and Doe have caused tortious injury by acts in this Commonwealth; and have caused tortious injury in this Commonwealth by acts and omissions outside this Commonwealth and regularly do or solicit business, or engage in any other persistent course of conduct.

10. Venue is appropriate in this Court pursuant to Virginia Code § 8.01-262. In addition, KBE contractually consented to venue in this Court in the MSA.

Facts

The New gTLD Program

11. In 2008, the Internet Corporation for Assigned Names and Numbers ("ICANN") approved a program for the launch of new generic top level domains ("gTLDs") in the Internet's addressing system. A top-level domain ("TLD") is, in simple terms, the letters to the right of the "dot" in a domain name, e.g., <.com> or <.org>. Unlike a country-code TLD ("ccTLD"), which generally is assigned to a country, sovereign state or dependent territory (e.g., <.uk>, <.cn>), a gTLD is one associated with a "generic" term such as <.com> or <.org>.

12. As part of ICANN's new gTLD program, persons and entities were permitted to apply, for a fee, for the rights to serve as the exclusive registry for proposed gTLDs. Some of these applicants were brand owners, seeking a gTLD for their brands (e.g., <.bmw>, <.suzuki>). Others applied for gTLDs that might have a broad appeal (e.g., <.web>), while others applied for gTLDs that might appeal to groups with special interests (e.g., <.attorney>, <.tires>).

13. Each applicant for a gTLD was required to demonstrate to ICANN that it was able to provide technically competent registry services for its proposed gTLD.

14. Verisign is, and has since 2000 been, the registry operator for the largest gTLD, <.com>, together with a number of other TLDs. For some of these TLDs such as <.com> and <.net>, Verisign has direct agreements with ICANN to operate the registries. In other cases, Verisign operates the registries under agreements with the parties authorized to operate the TLD (e.g., <.gov>, <.tv>).

15. As a result of Verisign's expertise as a registry operator, it has entered into agreements with applicants for some of the new gTLDs to provide certain back-end registry services for the applicants' new gTLDs.

The KBE Agreements

16. On April 12, 2012, Key Brand entered into a "Verisign Master Services Agreement" ("MSA") with Verisign, which set forth various terms relating to Verisign's general provision of services to Key Brand and its Affiliates (as that term is defined in the MSA), and contemplated service orders between Verisign and Key Brand and its Affiliates.

17. On April 12, 2012, KBE Holding entered into a "Verisign New gTLD Services SO" Service Order (the "Service Order") with Verisign which, in conjunction with the MSA, sets forth various terms relating to Verisign's provision of "New gTLD Services" (as defined in the Service Order) with respect to KBE's applied-for gTLDs.

18. Under the terms of the Service Order, Key Brand agreed to "guarantee[] the performance and payment obligations of KBE [] under the MSA, this SO, and each order form hereunder."

19. Pursuant to, and attached to, the Service Order, KBE executed and delivered order forms with respect the gTLDs <.broadway>, <.bway>, <.theater>, and <.theatre>.

20. On June 13, 2012, KBE applied to ICANN to be the registry operator for all four of these applied-for gTLDs.

21. KBE subsequently withdrew its applications for the <.broadway>, <.bway>, and <.theater> gTLDs. As a result, the parties' obligations under the MSA and the Service Order with respect thereto were terminated.

22. Pursuant to the MSA and the Service Order, KBE purchased Verisign's New gTLD Services (as defined in the Agreement) for the gTLD <.theatre> (hereinafter, the "KBE gTLD").

23. The Service Order also incorporates by reference the Service Guide for New gTLD Services (the "Service Guide"), which is attached to the Service Order.

24. The Service Guide provides that KBE "shall not change any information, data or document provided by Verisign or fail to use the responses provided by Verisign for the questions regarding Technical and Operational Capability of the TLD (as described herein) [in its applications with ICANN] without Verisign's prior written consent."

The KBE Application

25. On or about June 13, 2012, KBE submitted its initial application for the KBE gTLD to ICANN.[1] A copy of this application is attached hereto, incorporated herein, and marked as *Exhibit 1*.

26. As required by the Service Order, KBE's initial application to ICANN for the KBE gTLD identified Verisign as the exclusive provider of back-end registry

[1] This application states that the applicant is "Key GTLD Holding, Inc." This appears to be a typographical error.

services for the KBE gTLD, and included Verisign's specifications and responses regarding technical and operational capability of the KBE gTLD that Verisign previously provided to KBE pursuant to the terms of the Service Order.

27. KBE's application to ICANN for the KBE gTLD passed ICANN's initial evaluation process on June 7, 2013.

28. On or about October 10, 2014, KBE submitted to ICANN a request to change its application for the KBE gTLD. A copy of this change request is attached hereto, incorporated herein, and marked as *Exhibit 2*.

29. In its change request attached hereto as *Exhibit 2*, KBE removed the reference to Verisign as the provider of back-end registry services, and deleted Verisign's specifications and responses regarding technical and operational capability of the KBE gTLD.

30. In its change request attached hereto as *Exhibit 2*, KBE identified CentralNic as the provider of back-end registry services, and substituted CentralNic's specifications and responses regarding technical and operational capability of the KBE gTLD where Verisign's previously had appeared.

31. ICANN approved KBE's change request on December 19, 2014.

Why KBE Deleted Verisign From its Application

32. KBE has decided to sell and transfer their application for the KBE gTLD to a third party, Doe.

33. Upon information and belief, derived from statements made by KBE and Matter Strategic, KBE, acting in concert with advisors MJRC and Matter Strategic,

determined that the value of the applications in connection with Doe's proposed acquisition of the rights to the application for the KBE gTLD would be increased by eliminating Verisign as the provider of back-end registry services.

34. Upon information and belief, the sale and transfer of the rights to the applications for the KBE gTLD by KBE is imminent.

35. Upon information and belief, either (a) KBE has entered into an agreement with CentralNic to provide back-end registry services for the KBE gTLD that is intended to be assigned by KBE to Doe; or (b) Doe has entered into an agreement or arrangement with CentralNic as the provider of back-end registry services for the KBE gTLD in the event the application is transferred to Doe.

Count 1
Breach of Contract – KBE

36. The allegations in paragraphs 1 through 35 are incorporated herein as if fully set forth.

37. The MSA is a contract between Verisign and Key Brand.

38. The Service Order is a contract between Verisign and Key Brand and KBE Holdings, and Key Brand has guaranteed KBE Holdings' performance and payment obligations thereunder and under all service orders.

39. Under the Service Guide, which is part of the Service Order, KBE agreed not to change any information, data or document provided by Verisign, and not to fail to use the responses provided by Verisign for the questions regarding Technical and

Operational Capability of the TLD in their applications with ICANN, without Verisign's prior written consent.

40. Verisign never has expressly or impliedly consented to KBE changing any information, data or document provided by Verisign or using responses other than those provided by Verisign for the questions regarding Technical and Operational Capability of the TLD in its application with ICANN.

41. However, in its change request attached hereto as *Exhibit 2*, KBE removed references to Verisign as the provider of back-end registry services, and deleted Verisign's specifications and responses regarding technical and operational capability of the KBE gTLD.

42. The foregoing constitutes a breach of contract by KBE.

43. As a result of KBE's breach of contract as aforesaid, Verisign has and will continue to suffer damages.

44. Verisign lacks a complete and adequate remedy at law, and will be irreparably harmed if KBE is permitted to sell or transfer the application for the KBE gTLD using a different provider of back-end registry services in contravention of their obligation to exclusively use Verisign.

WHEREFORE, Verisign requests:

a. That judgment be entered in its favor, and against KBE Holdings and Key Brand, jointly and severally, in the principal sum of $175,000, plus prejudgment and post judgment interest, plus costs;

b. That Key Brand and KBE Holdings be preliminarily and permanently enjoined from selling, transferring or otherwise conveying the application for the KBE gTLD to any person or entity, including Doe; and

c. That the Court afford it such other and further relief as may be appropriate.

Count 2
Tortious Interference with Contract – CentralNic, Matter Strategic and Doe

45. The allegations in paragraphs 1 through 44 are incorporated herein as if fully set forth.

46. The MSA and Service Order were and are valid contracts between Verisign and Key Brand and KBE Holdings.

47. Upon information and belief, CentralNic, Matter Strategic and Doe, at all times relevant hereto, knew of the existence of the MSA and Service Order, and that Key Brand and KBE Holdings were and are obligated to use Verisign as the exclusive provider of back-end registry services for the KBE gTLD.

48. Upon information and belief, CentralNic, Matter Strategic and Doe intentionally, willfully and knowingly caused and induced Key Brand and KBE Holdings to breach the MSA and Service Order by replacing Verisign with CentralNic as the provider of back-end registry services in the applications for the KBE gTLD, so that Matter Strategic and Doe could better profit from the sale and transfer of the application to Doe, and so CentralNic could obtain a profitable contract.

49. As a result of CentralNic's, Matter Strategic's and Doe's tortious interference with Verisign's contracts with KBE and Key Brands, Verisign has and will continue to suffer damages.

50. Verisign lacks a complete and adequate remedy at law, and will be irreparably harmed if CentralNic were permitted to perform the services that are exclusively reserved to Verisign; if Matter Strategic were permitted to continue to provide advisory services and assist Key Brand, KBE Holdings and Doe with respect to a transaction that is violative of Verisign's contractual rights; and if Doe were permitted to purchase or accept the transfer of the application for the KBE gTLD.

WHEREFORE, Verisign requests:

a. That judgment be entered in its favor, and against CentralNic, Matter Strategic and Doe, jointly and severally, in the principal sum of $175,000, plus prejudgment and post judgment interest, plus costs, plus its attorneys' fees;

b. That CentralNic be preliminarily and permanently enjoined from providing back-end registry services in the application for the KBE gTLD;

c. That Matter Strategic be preliminarily and permanently enjoined from assisting Key Brand, KBE Holdings and/or Doe with respect to any transaction involving the sale, purchase, transfer or conveyance of the application for the KBE gTLD to any person or entity;

d. That Doe be preliminarily and permanently enjoined from purchasing, accepting transfer, or otherwise participating in conveying the application for the KBE gTLD to any person or entity; and

e. That the Court afford it such other and further relief as may be appropriate.

Count 3
Business Conspiracy (Va. Code §§ 18.2-499, -500) – All Defendants

51. The allegations in paragraphs 1 through 50 are incorporated herein as if fully set forth.

52. Key Brand, KBE Holdings, Matter Strategic and Doe and, upon information and belief, CentralNic, combined, associated, agreed, mutually undertook and concerted together for the purpose of willfully and maliciously injuring Verisign in its business, by seeking to circumvent Key Brands' and KBE Holdings' contractual requirements; by undermining Verisign's contractual right to be the exclusive provider of back-end registry services for the KBE gTLD; and by breaching and inducing breaches of the MSA and Service Order.

53. As a result of Key Brand's, KBE Holdings', CentralNic's, Matter Strategic's and Doe's conspiracy as aforesaid and Doe's tortious interference with Verisign's contracts with KBE Holdings and Key Brands, Verisign has and will continue to suffer damages.

54. Pursuant to Va. Code § 18.2-500, Verisign is entitled to recover treble damages, costs, attorneys' fees, and is also entitled to injunctive relief.

WHEREFORE, Verisign requests:

a. That judgment be entered in its favor, and against KBE Holdings, Key Brand, CentralNic, Matter Strategic and Doe, jointly and severally, in the

principal sum of $525,000, plus prejudgment and post judgment interest, plus costs, plus its attorneys' fees;

b. That KBE Holdings, Key Brand, CentralNic, Matter Strategic and Doe be enjoined from participating in any combination, association, agreement, mutual undertaking or concerted action injuring Verisign in its business;

c. That Key Brand and KBE Holdings be preliminarily and permanently enjoined from selling, transferring or otherwise conveying the application for the KBE gTLD to any person or entity, including Doe; and

d. That CentralNic be preliminarily and permanently enjoined from providing back-end registry services in the application for the KBE gTLD;

e. That Matter Strategic be preliminarily and permanently enjoined from assisting Key Brand, KBE Holdings and/or Doe with respect to any transaction involving the sale, purchase, transfer or conveyance of the application for the KBE gTLD to any person or entity;

f. That Doe be temporarily, preliminarily and permanently enjoined from purchasing, accepting transfer, or otherwise participating in conveying the application for the KBE gTLD to any person or entity; and

g. That the Court afford it such other and further relief as may be appropriate.

Demand for Attorneys' Fees

Pursuant to Rule 3:25, Verisign demands an award of its attorneys' fees, pursuant to Virginia Code § 18.2-500.

VERISIGN, INC.
By Counsel

HYLAND LAW PLLC
1818 Library Street, Suite 500
Reston, Virginia 20190
(703) 956-3566
Facsimile (703) 935-0349
Email thyland@hylandpllc.com
edwyer@hylandpllc.com

By: _____
Timothy B. Hyland (VSB No. 31163)
Elizabeth A. Dwyer (VSB No. 87486)
Counsel for Verisign

EXHIBIT 1

New gTLD Application Submitted to ICANN by: Key GTLD Holding Inc

String: theatre

Originally Posted: 13 June 2012

Application ID: 1-1326-3558

Applicant Information

1. Full legal name

Key GTLD Holding Inc

2. Address of the principal place of business

1619 Broadway
19th FLoor
New York NY 10019
UA

3. Phone number

0019174215467

4. Fax number

5. If applicable, website or URL

Primary Contact

6(a). Name

Matthew Russotti

6(b). Title

Consultant

6(c). Address

6(d). Phone Number

513 745 2810

6(e). Fax Number

6(f). Email Address

mrussotti@wolfe-sbmc.com

Secondary Contact

7(a). Name

Ms. Laurie Kunkel

7(b). Title

Consultant

7(c). Address

7(d). Phone Number

513 746 2800

7(e). Fax Number

7(f). Email Address

lkunkel@wolfe-sbmc.com

Proof of Legal Establishment

8(a). Legal form of the Applicant

Corporation

8(b). State the specific national or other jursidiction that defines the type of entity identified in 8(a).

Delaware

8(c). Attach evidence of the applicant's establishment.

Attachments are not displayed on this form.

9(a). If applying company is publicly traded, provide the exchange and symbol.

9(b). If the applying entity is a subsidiary, provide the parent company.

Key Brand Entertainment

9(c). If the applying entity is a joint venture, list all joint venture partners.

Applicant Background

11(a). Name(s) and position(s) of all directors

John Gore	President and Chief Financial Officer

11(b). Name(s) and position(s) of all officers and partners

John Gore	President and Chief Financial Officer
Liam Lynch	Executive Vice President
Seth Popper	Secretary
ThomasC. McGrath	Assistant Secretary

11(c). Name(s) and position(s) of all shareholders holding at least 15% of shares

11(d). For an applying entity that does not have directors, officers, partners, or shareholders: Name(s) and position(s) of all individuals having legal or executive responsibility

Applied-for gTLD string

13. Provide the applied-for gTLD string. If an IDN, provide the U-label.

theatre

14(a). If an IDN, provide the A-label (beginning with "xn--").

14(b). If an IDN, provide the meaning or restatement of the string in English, that is, a description of the literal meaning of the string in the opinion of the applicant.

14(c). If an IDN, provide the language of the label (in English).

14(c). If an IDN, provide the language of the label (as referenced by ISO-639-1).

14(d). If an IDN, provide the script of the label (in English).

14(d). If an IDN, provide the script of the label (as referenced by ISO 15924).

14(e). If an IDN, list all code points contained in the U-label according to Unicode form.

15(a). If an IDN, Attach IDN Tables for the proposed registry.

Attachments are not displayed on this form.

15(b). Describe the process used for development of the IDN tables submitted, including consultations and sources used.

15(c). List any variant strings to the applied-for gTLD string according to the relevant IDN tables.

16. Describe the applicant's efforts to ensure that there are no known operational or rendering problems concerning the applied-for gTLD string. If such issues are known, describe steps that will be taken to mitigate these issues in software and other applications.

Applicant's gTLD application is a non-IDN application. Applicant is unaware of any known operational or rendering problems related to the applied for gTLD.

17. (OPTIONAL) Provide a representation of the label according to the International Phonetic Alphabet (http://www.langsci.ucl.ac.uk/ipa/).

Mission/Purpose

18(a). Describe the mission/purpose of your proposed gTLD.

The mission of .theatre is to provide diverse internet users an enhanced online experience while enriching society with artistic and cultural diversity through high quality content, information and authentic connected experiences centered on live theatre, musicals, opera, ballet and other performing arts, Broadway, and other related concepts, topics and activities. .theatre will be a branded top level domain operated by KBE GTLD Holding Inc., a wholly-owned subsidiary of Key Brand Entertainment (KBE), and intends to function, per the ICANN-Registry Operator Registry Agreement, as a Specification 9 exempt system that will seek to provide internet users with the confidence that all of the programming, information, social media, shopping and/or lifestyle opportunities found on the .theatre branded top level domain is authentic, genuine, safe, trusted, and secure and affiliated with the KBE's broadway.com brand.

18(b). How do you expect that your proposed gTLD will benefit registrants, Internet users, and others?

The goal of .theatre is to provide high quality, authentic information and online experiences for individuals interested in live theatre, musicals, opera, ballet and other performing arts, Broadway, and other related concepts, topics and activities. The reputation of KBE, through its operation of broadway.com, is well recognized as a single source for high quality access to tickets, content, information and programming related to live theatre around the globe. The level of service to its customers is highly regarded as the single most trusted source for Broadway and live theatre entertainment.

Internet users will benefit because .theatre will provide an enhanced online experience from the existing broadway.com through its ability to build more personalized experiences for internet users seeking artistic and cultural diversity. .theatre will provide Applicant greater control over the domain as a registry operator, enabling the domain to be operated with the same exceptional values KBE has shown to users through the operation of broadway.com. Additionally, new communities can be identified and formed to connect internet users with others interested in theatre and other performing arts, Broadway and entertainment.

.theatre intends to function, per the ICANN-Registry Operator Registry Agreement, as a Specification 9 exempt system and will carefully monitor and safeguard the user experience to provide users confidence that they have found the well-known, famous brand associated with broadway.com, and can be certain that users will find the high quality content, information and experiences associated with a brand they know and trust. New users will quickly come to recognize that .theatre stands for authentic, high quality, trusted sources for information about live theatre and other performing arts, entertainment, experiences, products and services.

.theatre will provide users who navigate within .theatre privacy protection similar to what is currently provided on broadway.com. Applicant will annually review and audit these policies to ensure that best practices are being utilized to protect the safety, security and confidentiality of its users.

.theatre will further enhance brand consistency by creating numerous subdomains under the .theatre TLD that have not been available under the existing top level domain namespace. Further, the .theatre TLD creates the possibility that these to-be-created subdomains will be more precisely targeted to internet users that will use them, more focused on content associated with the TLD under which they will reside, and more relevant to the TLD.

18(c). What operating rules will you adopt to eliminate or minimize social costs?

.theatre intends to function, per the ICANN-Registry Operator Registry Agreement, as a Specification 9 exempt system. All second level domains will be for the benefit of .theatre users and its affiliates. All other subdomain names intended to be used within .theatre registry will be controlled and managed by KBE GTLD Holding Inc., for the benefit of itself or affiliates.

It is the intent of the Applicant to request an exemption from the new gTLD Code of Conduct per Section 6 of Specification 9 of the Registry Operator Code of Conduct. As such, Applicant intends to function in such a way that all domain name registrations in the TLD shall be registered to and maintained by Applicant and Applicant will not sell, distribute or transfer control of domain name registrations to any party that is not an Affiliate of Applicant as defined in the ICANN-Registry Operator Registry Agreement. All domain name registrations intended to be used within Applicant's registry will be registered to and controlled and

maintained by Applicant and for the benefit of Applicant and its users, parents, sisters and Affiliates.

In the event that Applicant is not granted an exemption from Specification 9, Applicant will partner with a corporate registrar with expertise in running a registry to support such efforts. Applicant intends to partner with its current corporate registrar or one of similar technical capability and expertise and allocate the appropriate funds and human resources to ensure that both itself, as the registry operator, and its selected registrar are at all times in compliance with ICANN guidelines.

Community-based Designation

19. Is the application for a community-based TLD?

No

20(a). Provide the name and full description of the community that the applicant is committing to serve.

20(b). Explain the applicant's relationship to the community identified in 20 (a).

20(c). Provide a description of the community-based purpose of the applied-for gTLD.

20(d). Explain the relationship between the applied-for gTLD string and the community identified in 20(a).

20(e). Provide a description of the applicant's intended registration policies in support of the community-based purpose of the applied-for gTLD.

20(f). Attach any written endorsements from institutions/groups representative of the community identified in 20(a).

Attachments are not displayed on this form.

Geographic Names

21(a). Is the application for a geographic name?

No

Protection of Geographic Names

22. Describe proposed measures for protection of geographic names at the second and other levels in the applied-for gTLD.

The Applicant will initially reserve country names from use in the second and other levels of the TLD, and other such names designated by ICANN and pursuant to Specification 5 and ICANN's ongoing policies and regulations. In this regard, Applicant will at all times comply with ICANN's geographic and all other reservation requirements as outlined in the Registry Agreement and Applicant's reserved name list mentioned below. Applicant's TLD will be operated as a Specification 9 exempt system, and the Applicant may, over time, utilize the reserved country names in the second and other country levels in order to organize content within the domain in a meaningful way. However, in such event, before the Applicant begins using such initially reserved country names, Applicant will provide a window during which governments, ICANN, public authorities or IGOs may submit a demand to block names with national or geographic significance at the second level of the TLD at no cost to the blocking authority. In the event of such occurrence, Applicant will at all times comply with all ICANN mandates and shall establish a notice mechanism and blocking procedure to effectuate such action.

All geographic and geopolitical names contained in the ISO 3166-1 list from time to time shall initially be reserved at both the second level and at all other levels within the TLD at which the Applicant provides for registrations. All names shall be reserved both in English and in all related official languages as may be directed by ICANN or the GAC. In addition, Applicant shall reserve names of territories, distinct geographic locations, and other geographic and geopolitical names as ICANN may direct from time to time. Such names shall be reserved from registration during any sunrise period, and shall be registered in ICANN's name prior to start-up and open registration in the TLD. Applicant shall post and maintain an updated listing of all such names on its website, which list shall be subject to change at ICANN's direction. Upon determination by ICANN of appropriate standards and qualifications for registration following input from interested parties in the Internet community, such names may be approved for registration to the appropriate authoritative body.

Pursuant to any ICANN directive allowing release after the blocking period has concluded, a contact will be delegated and information posted to enable governments, public authorities, or IGOs to challenge abuses of names with national or geographic significance at the second level of the TLD during the operation of the TLD. Challenges will be reviewed on their merits and resolved in a way that demonstrates that the Applicant respects sensitivities regarding terms with national, cultural, geographic and religious significance while enabling Applicant to provide content to users in a logical and organized fashion.

Additionally, Verisign, as Applicant's back-end registry provider, provides a mechanism through their registry solution for reserving second-level domain names that prevents them from being registered. This functionality includes a list of strings that the system will not allow to be registered. Strings can be added and removed from this list as needed.

For the protection of geographic names for the Applicant's TLD, the country and territory names contained in the following internationally recognized lists shall be blocked initially:

* The short form (in English) of all country and territory names, including the European Union, contained on the International Organization for Standardization (ISO) 3166-1 list located at: http://www.iso.org/iso/support/country_codes/iso_3166_code_lists/iso-3166-1_decoding_table.htm#EU

* The United Nations Group of Experts on Geographical Names (UNGEGN), Technical Reference Manual for the Standardization of Geographical Names, Part III Names of Countries of the World: http://unstats.un.org/unsd/geoinfo/UNGEGN/publications.html

* The list of United Nations member states, in six official United Nations languages, prepared by the Working Group on Country Names of the United Nations Conference on the Standardization of Geographical Names. The most recent list of country names approved by the Working Group was submitted on behalf of UNGEGN for the Ninth UN Conference on the Standardization of Geographical Names in August 2007: E/CONF.98/89 Add.1 http://unstats.un.org/unsd/geoinfo/ungegn/docs/9th-uncsgn-docs/econf/9th_UNCSGN_e-conf-98-89-add1.pdf

As new versions of these three internationally recognized lists are published, Verisign will update the list of names reserved by the Verisign registry system to reflect any changes.

In addition to providing protection for geographic names, this reserved name functionality will be used to reserve other names specifically ineligible for delegation.

For example, Section 2.2.1.2.3 of the Applicant Guidebook lists strings associated with the International Olympic Committee and the International Red Cross and Red Crescent organizations to be prohibited from delegation per the Government Advisory Committee (GAC) request.

All the strings on these lists as well as any others put forth by the GAC and approved by ICANN will be included in the list of reserved names.

There are no plans at this time to release any of the reserved names. If, however, Applicant intends to release any of the names at a future date, we will follow the appropriate procedures, outlined in Section 5 of Specification 5, on the release of reserved names.

Registry Services

23. Provide name and full description of all the Registry Services to be provided.

1 CUSTOMARY REGISTRY SERVICES

As the Applicant's selected provider of backend registry services, Verisign provides a comprehensive system and physical security solution that is designed to ensure a TLD is protected from unauthorized disclosure, alteration, insertion, or destruction of registry data. Verisign's system addresses all areas of security including information and policies, security procedures, the systems development lifecycle, physical security, system hacks, break-ins, data tampering, and other disruptions to operations. Verisign's operational environments not only meet the security criteria specified in its customer contractual agreements, thereby preventing unauthorized access to or disclosure of information or resources on the Internet by systems operating in accordance with applicable standards, but also are subject to multiple independent assessments as detailed in the response to Question 30, Security Policy. Verisign's physical and system security methodology follows a mature, ongoing lifecycle that was developed and implemented many years before the development of the industry standards with which Verisign currently complies. Please see the response to Question 30, Security Policy, for details of the security features of Verisign's registry services.

Verisign's registry services fully comply with relevant standards and best current practice RFCs published by the Internet Engineering Task Force (IETF), including all successor standards, modifications, or additions relating to the DNS and name server operations including without limitation RFCs 1034, 1035, 1982, 2181, 2182, 2671, 3226, 3596, 3597, 3901, 4343, and 4472. Moreover, Verisign's Shared Registration System (SRS) supports the following IETF Extensible Provisioning Protocol (EPP) specifications, where the Extensible Markup Language (XML) templates and XML schemas are defined in RFC 3915, 5730, 5731, 5732, 5733, and 5734. By strictly adhering to these RFCs, Verisign helps to ensure its registry services do not create a condition that adversely affects the throughput, response time, consistency, or coherence of responses to Internet servers or end systems. Besides its leadership in authoring RFCs for EPP, Domain Name System Security Extensions (DNSSEC), and other DNS services, Verisign has created and contributed to several now well-established IETF standards and is a regular and long-standing participant in key Internet standards forums.

Figure 23 1 summarizes the technical and business components of those registry services, customarily offered by a registry operator (i.e., Verisign), that support this application. These services are currently operational and support both large and small Verisign-managed registries. Customary registry services are provided in the same manner as Verisign provides these services for its existing gTLDs. Through these established registry services, Verisign has proven its ability to operate a reliable and low-risk registry that supports millions of transactions per day. Verisign is unaware of any potential security or stability concern related to any of these services.

Registry services defined by this application are not intended to be offered in a manner unique to the new generic top-level domain (gTLD) nor are any proposed services unique to this application's registry.

As further evidence of Verisign's compliance with ICANN mandated security and stability requirements, Verisign allocates the applicable RFCs to each of the five customary registry services (items A - E above). For each registry service, Verisign also provides evidence in Figure 23 2 of Verisign's RFC compliance and includes relevant ICANN prior-service approval actions.

1.1 Critical Operations of the Registry

i. Receipt of Data from Registrars Concerning Registration of Domain Names and Name Servers
See Item A in Figure 23 1 and Figure 23 2.
ii. Provision to Registrars Status Information Relating to the Zone Servers
Verisign is the Applicant's selected provider of backend registry services. Verisign registry services provisions to registrars status information relating to zone servers for the TLD. The services also allow a domain name to be updated with clientHold, serverHold status, which removes the domain name server details from zone files. This ensures that DNS queries of the domain name are not resolved temporarily. When these hold statuses are removed, the name server details are written back to zone files and DNS queries are again resolved. Figure 23 3 describes the domain name status information and zone insertion indicator provided to registrars. The zone insertion indicator determines whether the name server details of the domain name exist in the zone file for a given domain name status. Verisign also has the capability to withdraw domain names from the zone file in near-real time by changing the domain name statuses upon request by customers, courts, or legal authorities as required.
iii. Dissemination of TLD Zone Files
See Item B in Figure 23 1 and Figure 23 2.
iv. Operation of the Registry Zone Servers
Verisign is the Applicant's selected provider of backend registry services. Verisign, as a company, operates zone servers and serves DNS resolution from 76 geographically distributed resolution sites located in North America, South America, Africa, Europe, Asia, and Australia. Currently, 17 DNS locations are designated primary sites, offering greater capacity than smaller sites comprising the remainder of the Verisign constellation. Verisign also uses Anycast techniques and regional Internet resolution sites to expand coverage, accommodate emergency or surge capacity, and support system availability during maintenance procedures. Verisign operates the Applicant's gTLD from a minimum of eight of its primary sites (two on the East Coast of the United States, two on the West Coast of the United States, two in Europe, and two in Asia) and expands resolution sites based on traffic volume and patterns. Further details of the geographic diversity of Verisign's zone servers are provided in the response to Question 34, Geographic Diversity. Moreover, additional details of Verisign's zone servers are provided in the response to Question 32, Architecture and the response to Question 35, DNS Service.
v. Dissemination of Contact and Other Information Concerning Domain Name Server Registrations
See Item C in Figure 23 1 and Figure 23 2.
2 OTHER PRODUCTS OR SERVICES THE REGISTRY OPERATOR IS REQUIRED TO PROVIDE BECAUSE OF THE ESTABLISHMENT OF A CONSENSUS POLICY
Verisign, the Applicant's selected provider of backend registry services, is a proven supporter of ICANN's consensus-driven, bottom-up policy development process whereby community members identify a problem, initiate policy discussions, and generate a solution that produces effective and sustained results. Verisign currently provides all of the products or services (collectively referred to as services) that the registry operator is required to provide because of the establishment of a Consensus Policy. For this TLD, Verisign implements these services using the same proven processes and procedures currently in-place for all registries under Verisign's management. Furthermore, Verisign executes these services on computing platforms comparable to those of other registries under Verisign's management. Verisign's extensive experience with consensus policy required services and its proven processes to implement these services greatly minimize any potential risk to Internet security or stability. Details of these services are provided in the following subsections. It shall be noted that consensus policy services required of registrars (e.g., Whois Reminder, Expired Domain) are not included in this response. This exclusion is in accordance with the direction provided in the question's Notes column to address registry operator services.
2.1 Inter-Registrar Transfer Policy (IRTP)
Technical Component: In compliance with the IRTP consensus policy, Verisign, the

Applicant's selected provider of backend registry services, has designed its registration systems to systematically restrict the transfer of domain names within 60 days of the initial create date. In addition, Verisign has implemented EPP and "AuthInfo" code functionality, which is used to further authenticate transfer requests. The registration system has been designed to enable compliance with the five-day Transfer grace period and includes the following functionality:

- Allows the losing registrar to proactively 'ACK' or acknowledge a transfer prior to the expiration of the five-day Transfer grace period
- Allows the losing registrar to proactively 'NACK' or not acknowledge a transfer prior to the expiration of the five-day Transfer grace period
- Allows the system to automatically ACK the transfer request once the five-day Transfer grace period has passed if the losing registrar has not proactively ACK'd or NACK'd the transfer request.

Business Component: All requests to transfer a domain name to a new registrar are handled according to the procedures detailed in the IRTP. Dispute proceedings arising from a registrar's alleged failure to abide by this policy may be initiated by any ICANN-accredited registrar under the Transfer Dispute Resolution Policy. Applicant's compliance office serves as the first-level dispute resolution provider pursuant to the associated Transfer Dispute Resolution Policy. As needed Verisign is available to offer policy guidance as issues arise.

Security and Stability Concerns: Verisign is unaware of any impact, caused by the service, on throughput, response time, consistency, or coherence of the responses to Internet servers or end-user systems. By implementing the IRTP in accordance with ICANN policy, security is enhanced as all transfer commands are authenticated using the AuthInfo code prior to processing.

ICANN Prior Approval: Verisign has been in compliance with the IRTP since November 2004 and is available to support the Applicant in a consulting capacity as needed.

Unique to the TLD: This service is not provided in a manner unique to this TLD.

2.2 Add Grace Period (AGP) Limits Policy

Technical Component: Verisign's registry system monitors registrars' Add grace period deletion activity and provides reporting that permits the Applicant to assess registration fees upon registrars that have exceeded the AGP thresholds stipulated in the AGP Limits Policy. Further, Applicant accepts and evaluates all exemption requests received from registrars and determines whether the exemption request meets the exemption criteria. Applicant maintains all AGP Limits Policy exemption request activity so that this material may be included within Applicant's Monthly Registry Operator Report to ICANN.

Registrars that exceed the limits established by the policy may submit exemption requests to the applicant for consideration. Applicant's compliance office reviews these exemption requests in accordance with the AGP Limits Policy and renders a decision. Upon request, the applicant submits associated reporting on exemption request activity to support reporting in accordance with established ICANN requirements.

Business Component: The Add grace period (AGP) is restricted for any gTLD operator that has implemented an AGP. Specifically, for each operator:

- During any given month, an operator may not offer any refund to an ICANN-accredited registrar for any domain names deleted during the AGP that exceed (i) 10% of that registrar's net new registrations (calculated as the total number of net adds of one-year through ten-year registrations as defined in the monthly reporting requirement of Operator Agreements) in that month, or (ii) fifty (50) domain names, whichever is greater, unless an exemption has been granted by an operator.
- Upon the documented demonstration of extraordinary circumstances, a registrar may seek from an operator an exemption from such restrictions in a specific month. The registrar must confirm in writing to the operator how, at the time the names were deleted, these extraordinary circumstances were not known, reasonably could not have been known, and were outside the registrar's control. Acceptance of any exemption will be at the sole and reasonable discretion of the operator; however "extraordinary circumstances" that reoccur regularly for the same registrar will not be deemed extraordinary.

In addition to all other reporting requirements to ICANN, the Applicant identifies each registrar that has sought an exemption, along with a brief description of the type of extraordinary circumstance and the action, approval, or denial that the operator took.
Security and Stability Concerns: Verisign is unaware of any impact, caused by the policy, on throughput, response time, consistency, or coherence of the responses to Internet servers or end-user systems.
ICANN Prior Approval: Verisign, the applicant's backend registry services provider, has had experience with this policy since its implementation in April 2009 and is available to support the applicant in a consulting capacity as needed.
Unique to the TLD: This service is not provided in a manner unique to this TLD.
2.3 Registry Services Evaluation Policy (RSEP)
Technical Component: Verisign, the Applicant's selected provider of backend registry services, adheres to all RSEP submission requirements. Verisign has followed the process many times and is fully aware of the submission procedures, the type of documentation required, and the evaluation process that ICANN adheres to.
Business Component: In accordance with ICANN procedures detailed on the ICANN RSEP website (http://www.icann.org/en/registries/rsep/), all gTLD registry operators are required to follow this policy when submitting a request for new registry services.
Security and Stability Concerns: As part of the RSEP submission process, Verisign, Applicant's backend registry services provider, identifies any potential security and stability concerns in accordance with RSEP stability and security requirements. Verisign never launches services without satisfactory completion of the RSEP process and resulting approval.
ICANN Prior Approval: Not applicable.
Unique to the TLD: gTLD RSEP procedures are not implemented in a manner unique to this TLD.
3 PRODUCTS OR SERVICES ONLY A REGISTRY OPERATOR IS CAPABLE OF PROVIDING BY REASON OF ITS DESIGNATION AS THE REGISTRY OPERATOR
Verisign, the Applicant's selected backend registry services provider, has developed a Registry-Registrar Two-Factor Authentication Service that complements traditional registration and resolution registry services. In accordance with direction provided in Question 23, Verisign details below the technical and business components of the service, identifies any potential threat to registry security or stability, and lists previous interactions with ICANN to approve the operation of the service. The Two-Factor Authentication Service is currently operational, supporting multiple registries under ICANN's purview.
Applicant is unaware of any competition issue that may require the registry service (s) listed in this response to be referred to the appropriate governmental competition authority or authorities with applicable jurisdiction. ICANN previously approved the service(s), at which time it was determined that either the service(s) raised no competitive concerns or any applicable concerns related to competition were satisfactorily addressed.
3.1 Two-Factor Authentication Service
Technical Component: The Registry-Registrar Two-Factor Authentication Service is designed to improve domain name security and assist registrars in protecting the accounts they manage. As part of the service, dynamic one-time passwords augment the user names and passwords currently used to process update, transfer, and/or deletion requests. These one-time passwords enable transaction processing to be based on requests that are validated both by "what users know" (i.e., their user name and password) and "what users have" (i.e., a two-factor authentication credential with a one-time-password).
Registrars can use the one-time-password when communicating directly with Verisign's Customer Service department as well as when using the registrar portal to make manual updates, transfers, and/or deletion transactions. The Two-Factor Authentication Service is an optional service offered to registrars that execute the Registry-Registrar Two-Factor Authentication Service Agreement.
Business Component: There is no charge for the Registry-Registrar Two-Factor Authentication Service. It is enabled only for registrars that wish to take advantage of the added security provided by the service.

Security and Stability Concerns: Verisign is unaware of any impact, caused by the service, on throughput, response time, consistency, or coherence of the responses to Internet servers or end-user systems. The service is intended to enhance domain name security, resulting in increased confidence and trust by registrants.
ICANN Prior Approval: ICANN approved the same Two-Factor Authentication Service for Verisign's use on .com and .net on 10 July 2009 (RSEP Proposal 2009004) and for .name on 16 February 2011 (RSEP Proposal 2011001).
Unique to the TLD: This service is not provided in a manner unique to this TLD.

Demonstration of Technical & Operational Capability

24. Shared Registration System (SRS) Performance

1 ROBUST PLAN FOR OPERATING A RELIABLE SRS
1.1 High-Level Shared Registration System (SRS) System Description
Verisign, the Applicant's selected provider of backend registry services, provides and operates a robust and reliable SRS that enables multiple registrars to provide domain name registration services in the top-level domain (TLD). Verisign's proven reliable SRS serves approximately 915 registrars, and Verisign, as a company, has averaged more than 140 million registration transactions per day. The SRS provides a scalable, fault-tolerant platform for the delivery of gTLDs through the use of a central customer database, a web interface, a standard provisioning protocol (i.e., Extensible Provisioning Protocol, EPP), and a transport protocol (i.e., Secure Sockets Layer, SSL).
The SRS components include:
• Web Interface: Allows customers to access the authoritative database for accounts, contacts, users, authorization groups, product catalog, product subscriptions, and customer notification messages.
• EPP Interface: Provides an interface to the SRS that enables registrars to use EPP to register and manage domains, hosts, and contacts.
• Authentication Provider: A Verisign developed application, specific to the SRS, that authenticates a user based on a login name, password, and the SSL certificate common name and client IP address.
The SRS is designed to be scalable and fault tolerant by incorporating clustering in multiple tiers of the platform. New nodes can be added to a cluster within a single tier to scale a specific tier, and if one node fails within a single tier, the services will still be available. The SRS allows registrars to manage the TLD domain names in a single architecture.
To flexibly accommodate the scale of its transaction volumes, as well as new technologies, Verisign employs the following design practices:
• Scale for Growth: Scale to handle current volumes and projected growth.
• Scale for Peaks: Scale to twice base capacity to withstand "registration add attacks" from a compromised registrar system.
• Limit Database CPU Utilization: Limit utilization to no more than 50 percent during peak loads.
• Limit Database Memory Utilization: Each user's login process that connects to the database allocates a small segment of memory to perform connection overhead, sorting, and data caching. Verisign's standards mandate that no more than 40 percent of the total available physical memory on the database server will be allocated for these functions.
Verisign's SRS is built upon a three-tier architecture as illustrated in Figure 24 1 and detailed here:
• Gateway Layer: The first tier, the gateway servers, uses EPP to communicate with registrars. These gateway servers then interact with application

servers, which comprise the second tier.

- Application Layer: The application servers contain business logic for managing and maintaining the registry business. The business logic is particular to each TLD's business rules and requirements. The flexible internal design of the application servers allows Verisign to easily leverage existing business rules to apply to the TLD. The application servers store the Applicant's data in the registry database, which comprises the third and final tier. This simple, industry-standard design has been highly effective with other customers for whom Verisign provides backend registry services.
- Database Layer: The database is the heart of this architecture. It stores all the essential information provisioned from registrars through the gateway servers. Separate servers query the database, extract updated zone and Whois information, validate that information, and distribute it around the clock to Verisign's worldwide domain name resolution sites.

Scalability and Performance. Verisign, the Applicant's selected backend registry services provider, implements its scalable SRS on a supportable infrastructure that achieves the availability requirements in Specification 10. Verisign employs the design patterns of simplicity and parallelism in both its software and systems, based on its experience that these factors contribute most significantly to scalability and reliable performance. Going counter to feature-rich development patterns, Verisign intentionally minimizes the number of lines of code between the end user and the data delivered. The result is a network of restorable components that provide rapid, accurate updates. Figure 24 2 depicts EPP traffic flows and local redundancy in Verisign's SRS provisioning architecture. As detailed in the figure, local redundancy is maintained for each layer as well as each piece of equipment. This built-in redundancy enhances operational performance while enabling the future system scaling necessary to meet additional demand created by this or future registry applications.

Besides improving scalability and reliability, local SRS redundancy enables Verisign to take down individual system components for maintenance and upgrades, with little to no performance impact. With Verisign's redundant design, Verisign can perform routine maintenance while the remainder of the system remains online and unaffected. For the TLD registry, this flexibility minimizes unplanned downtime and provides a more consistent end-user experience.

1.2 Representative Network Diagrams

Figure 24 3 provides a summary network diagram of the Applicant's selected backend registry services provider's (Verisign's) SRS. This configuration at both the primary and alternate-primary Verisign data centers provides a highly reliable backup capability. Data is continuously replicated between both sites to ensure failover to the alternate-primary site can be implemented expeditiously to support both planned and unplanned outages.

1.3 Number of Servers

As the Applicant's selected provider of backend registry services, Verisign continually reviews its server deployments for all aspects of its registry service. Verisign evaluates usage based on peak performance objectives as well as current transaction volumes, which drive the quantity of servers in its implementations. Verisign's scaling is based on the following factors:

- Server configuration is based on CPU, memory, disk IO, total disk, and network throughput projections.
- Server quantity is determined through statistical modeling to fulfill overall performance objectives as defined by both the service availability and the server configuration.
- To ensure continuity of operations for the TLD, Verisign uses a minimum of 100 dedicated servers per SRS site. These servers are virtualized to meet demand.

1.4 Description of Interconnectivity with Other Registry Systems

Figure 24 4 provides a technical overview of the Applicant's selected backend registry services provider's (Verisign's) SRS, showing how the SRS component fits into this larger system and interconnects with other system components.

1.5 Frequency of Synchronization Between Servers

As Applicant's selected provider of backend registry services, Verisign uses

synchronous replication to keep the Verisign SRS continuously in sync between the two data centers. This synchronization is performed in near-real time, thereby supporting rapid failover should a failure occur or a planned maintenance outage be required.

1.6 Synchronization Scheme

Verisign uses synchronous replication to keep the Verisign SRS continuously in sync between the two data centers. Because the alternate-primary site is continuously up, and built using an identical design to the primary data center, it is classified as a "hot standby."

2 SCALABILITY AND PERFORMANCE ARE CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

Verisign is an experienced backend registry provider that has developed and uses proprietary system scaling models to guide the growth of its TLD supporting infrastructure. These models direct Verisign's infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. Verisign periodically updates these models to account for the adoption of more capable and cost-effective technologies.

Verisign's scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the TLD with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its scaling models, Verisign derived the necessary infrastructure required to implement and sustain this gTLD. Verisign's pricing for the backend registry services it provides to the Applicant fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

3 TECHNICAL PLAN THAT IS ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

Verisign, the Applicant's selected provider of backend registry services, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services provided to the Applicant fully accounts for this personnel-related cost, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign's quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign's ability to align personnel resource growth to the scale increases of Verisign's TLD service offerings.

Verisign projects it will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support SRS performance:

- Application Engineers: 19
- Database Administrators: 8
- Database Engineers: 3
- Network Administrators: 11
- Network Architects: 4

- Project Managers: 25
- Quality Assurance Engineers: 11
- SRS System Administrators: 13
- Storage Administrators: 4
- Systems Architects: 9

To implement and manage the TLD as described in this application, Verisign, the Applicant's selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.
When usage projections indicate a need for additional staff, Verisign's internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only this proposed gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

4 EVIDENCE OF COMPLIANCE WITH SPECIFICATION 6 AND 10 TO THE REGISTRY AGREEMENT

Section 1.2 (EPP) of Specification 6, Registry Interoperability and Continuity Specifications. Verisign, the Applicant's selected backend registry services provider, provides these services using its SRS, which complies fully with Specification 6, Section 1.2 of the Registry Agreement. In using its SRS to provide backend registry services, Verisign implements and complies with relevant existing RFCs (i.e., 5730, 5731, 5732, 5733, 5734, and 5910) and intends to comply with RFCs that may be published in the future by the Internet Engineering Task Force (IETF), including successor standards, modifications, or additions thereto relating to the provisioning and management of domain names that use EPP. In addition, Verisign's SRS includes a Registry Grace Period (RGP) and thus complies with RFC 3915 and its successors. Details of the Verisign SRS' compliance with RFC SRS/EPP are provided in the response to Question 25, Extensible Provisioning Protocol. Verisign does not use functionality outside the base EPP RFCs, although proprietary EPP extensions are documented in Internet-Draft format following the guidelines described in RFC 3735 within the response to Question 25. Moreover, prior to deployment, the Applicant will provide to ICANN updated documentation of all the EPP objects and extensions supported in accordance with Specification 6, Section 1.2.
Specification 10, EPP Registry Performance Specifications. Verisign's SRS meets all EPP Registry Performance Specifications detailed in Specification 10, Section 2. Evidence of this performance can be verified by a review of the .com and .net Registry Operator's Monthly Reports, which Verisign files with ICANN. These reports detail Verisign's operational status of the .com and .net registries, which use an SRS design and approach comparable to the one proposed for this TLD. These reports provide evidence of Verisign's ability to meet registry operation service level agreements (SLAs) comparable to those detailed in Specification 10. The reports are accessible at the following URL: http://www.icann.org/en/tlds/monthly-reports/.
In accordance with EPP Registry Performance Specifications detailed in Specification 10, Verisign's SRS meets the following performance attributes:

- EPP service availability: ≤ 864 minutes of downtime (≈98%)
- EPP session-command round trip time (RTT): ≤4000 milliseconds (ms), for at least 90 percent of the commands
- EPP query-command RTT: ≤2000 ms, for at least 90 percent of the commands
- EPP transform-command RTT: ≤4000 ms, for at least 90 percent of the commands

25. Extensible Provisioning Protocol (EPP)

1 COMPLETE KNOWLEDGE AND UNDERSTANDING OF THIS ASPECT OF REGISTRY TECHNICAL REQUIREMENTS

Verisign, the Applicant's selected backend registry services provider, has used Extensible Provisioning Protocol (EPP) since its inception and possesses complete knowledge and understanding of EPP registry systems. Its first EPP implementation—for a thick registry for the .name generic top-level domain (gTLD)—was in 2002. Since then Verisign has continued its RFC-compliant use of EPP in multiple TLDs, as detailed in Figure 25 1.

Verisign's understanding of EPP and its ability to implement code that complies with the applicable RFCs is unparalleled. Mr. Scott Hollenbeck, Verisign's director of software development, authored the Extensible Provisioning Protocol and continues to be fully engaged in its refinement and enhancement (U.S. Patent Number 7299299 - Shared registration system for registering domain names). Verisign has also developed numerous new object mappings and object extensions following the guidelines in RFC 3735 (Guidelines for Extending the Extensible Provisioning Protocol). Mr. James Gould, a principal engineer at Verisign, led and co-authored the most recent EPP Domain Name System Security Extensions (DNSSEC) RFC effort (RFC 5910).

All registry systems for which Verisign is the registry operator or provides backend registry services use EPP. Upon approval of this application, Verisign will use EPP to provide the backend registry services for this gTLD. The .com, .net, and .name registries for which Verisign is the registry operator use an SRS design and approach comparable to the one proposed for this gTLD. Approximately 915 registrars use the Verisign EPP service, and the registry system performs more than 140 million EPP transactions daily without performance issues or restrictive maintenance windows. The processing time service level agreement (SLA) requirements for the Verisign-operated .net gTLD are the strictest of the current Verisign managed gTLDs. All processing times for Verisign-operated gTLDs can be found in ICANN's Registry Operator's Monthly Reports at http://www.icann.org/en/tlds/monthly-reports/.

Verisign has also been active on the Internet Engineering Task Force (IETF) Provisioning Registry Protocol (provreg) working group and mailing list since work started on the EPP protocol in 2000. This working group provided a forum for members of the Internet community to comment on Mr. Scott Hollenbeck's initial EPP drafts, which Mr. Hollenbeck refined based on input and discussions with representatives from registries, registrars, and other interested parties. The working group has since concluded, but the mailing list is still active to enable discussion of different aspects of EPP.

1.1 EPP Interface with Registrars

Verisign, the Applicant's selected backend registry services provider, fully supports the features defined in the EPP specifications and provides a set of software development kits (SDK) and tools to help registrars build secure and stable interfaces. Verisign's SDKs give registrars the option of either fully writing their own EPP client software to integrate with the Shared Registration System (SRS), or using the Verisign-provided SDKs to aid them in the integration effort. Registrars can download the Verisign EPP SDKs and tools from the registrar website (http://www.Verisign.com/domain-name-services/current-registrars/epp-sdk/index.html).

The EPP SDKs provide a host of features including connection pooling, Secure Sockets Layer (SSL), and a test server (stub server) to run EPP tests against. One tool—the EPP tool—provides a web interface for creating EPP Extensible Markup Language (XML) commands and sending them to a configurable set of target servers. This helps registrars in creating the template XML and testing a variety of test cases against the EPP servers. An Operational Test and Evaluation (OT&E) environment, which runs the same software as the production system so approved registrars can integrate and test their software before moving into a live

production environment, is also available.

2 TECHNICAL PLAN SCOPE/SCALE CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

Verisign, the Applicant's selected backend registry services provider, is an experienced backend registry provider that has developed and uses proprietary system scaling models to guide the growth of its TLD supporting infrastructure. These models direct Verisign's infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. Verisign periodically updates these models to account for the adoption of more capable and cost-effective technologies.

Verisign's scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the TLD with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its scaling models, Verisign derived the necessary infrastructure required to implement and sustain this gTLD. Verisign's pricing for the backend registry services it provides to the Applicant fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

3 TECHNICAL PLAN THAT IS ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

Verisign, the Applicant's selected backend registry services provider, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services it provides to the Applicant fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign's quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign's ability to align personnel resource growth to the scale increases of Verisign's TLD service offerings.

Verisign projects it will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support the provisioning of EPP services:

- Application Engineers: 19
- Database Engineers: 3
- Quality Assurance Engineers: 11

To implement and manage the TLD as described in this application, Verisign, the Applicant's selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.

When usage projections indicate a need for additional staff, Verisign's internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to

manage only this proposed gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed TLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

4 ABILITY TO COMPLY WITH RELEVANT RFCS

Verisign, the Applicant's selected backend registry services provider, incorporates design reviews, code reviews, and peer reviews into its software development lifecycle (SDLC) to ensure compliance with the relevant RFCs. Verisign's dedicated QA team creates extensive test plans and issues internal certifications when it has confirmed the accuracy of the code in relation to the RFC requirements. Verisign's QA organization is independent from the development team within engineering. This separation helps Verisign ensure adopted processes and procedures are followed, further ensuring that all software releases fully consider the security and stability of the TLD.

For the TLD, the Shared Registration System (SRS) complies with the following IETF EPP specifications, where the XML templates and XML schemas are defined in the following specifications:

- EPP RGP 3915 (http://www.apps.ietf.org/rfc/rfc3915.html): EPP Redemption Grace Period (RGP) Mapping specification for support of RGP statuses and support of Restore Request and Restore Report (authored by Verisign's Scott Hollenbeck)
- EPP 5730 (http://tools.ietf.org/html/rfc5730): Base EPP specification (authored by Verisign's Scott Hollenbeck)
- EPP Domain 5731 (http://tools.ietf.org/html/rfc5731): EPP Domain Name Mapping specification (authored by Verisign's Scott Hollenbeck)
- EPP Host 5732 (http://tools.ietf.org/html/rfc5732): EPP Host Mapping specification (authored by Verisign's Scott Hollenbeck)
- EPP Contact 5733 (http://tools.ietf.org/html/rfc5733): EPP Contact Mapping specification (authored by Verisign's Scott Hollenbeck)
- EPP TCP 5734 (http://tools.ietf.org/html/rfc5734): EPP Transport over Transmission Control Protocol (TCP) specification (authored by Verisign's Scott Hollenbeck)
- EPP DNSSEC 5910 (http://tools.ietf.org/html/rfc5910): EPP Domain Name System Security Extensions (DNSSEC) Mapping specification (authored by Verisign's James Gould and Scott Hollenbeck)

5 PROPRIETARY EPP EXTENSIONS

Verisign, the Applicant's selected backend registry services provider, uses its SRS to provide registry services. The SRS supports the following EPP specifications, which Verisign developed following the guidelines in RFC 3735, where the XML templates and XML schemas are defined in the specifications:

- IDN Language Tag (http://www.verisigninc.com/assets/idn-language-tag.pdf): EPP internationalized domain names (IDN) language tag extension used for IDN domain name registrations
- RGP Poll Mapping (http://www.verisigninc.com/assets/whois-info-extension.pdf): EPP mapping for an EPP poll message in support of Restore Request and Restore Report
- Whois Info Extension (http://www.verisigninc.com/assets/whois-info-extension.pdf): EPP extension for returning additional information needed for transfers
- EPP ConsoliDate Mapping (http://www.verisigninc.com/assets/consolidate-mapping.txt): EPP mapping to support a Domain Sync operation for synchronizing domain name expiration dates
- NameStore Extension (http://www.verisigninc.com/assets/namestore-extension.pdf): EPP extension for routing with an EPP intelligent gateway to a pluggable set of backend products and services
- Low Balance Mapping (http://www.verisigninc.com/assets/low-balance-mapping.pdf): EPP mapping to support low balance poll messages that proactively

notify registrars of a low balance (available credit) condition
As part of the 2006 implementation report to bring the EPP RFC documents from Proposed Standard status to Draft Standard status, an implementation test matrix was completed. Two independently developed EPP client implementations based on the RFCs were tested against the Verisign EPP server for the domain, host, and contact transactions. No compliance-related issues were identified during this test, providing evidence that these extensions comply with RFC 3735 guidelines and further demonstrating Verisign's ability to design, test, and deploy an RFC-compliant EPP implementation.

5.1 EPP Templates and Schemas

The EPP XML schemas are formal descriptions of the EPP XML templates. They are used to express the set of rules to which the EPP templates must conform in order to be considered valid by the schema. The EPP schemas define the building blocks of the EPP templates, describing the format of the data and the different EPP commands' request and response formats. The current EPP implementations managed by Verisign, the Applicant's selected backend registry services provider, use these EPP templates and schemas, as will the proposed TLD. For each proprietary XML template/schema Verisign provides a reference to the applicable template and includes the schema.

XML templates/schema for idnLang-1.0

- Template: The templates for idnLang-1.0 can be found in Chapter 3, EPP Command Mapping of the relevant EPP documentation, http://www.verisigninc.com/assets/idn-language-tag.pdf.
- Schema: This schema describes the extension mapping for the IDN language tag. The mapping extends the EPP domain name mapping to provide additional features required for the provisioning of IDN domain name registrations.

```
<?xml version="1.0" encoding="UTF-8"?>

<schema targetNamespace="http://www.Verisign.com/epp/idnLang-1.0"
 xmlns:idnLang="http://www.Verisign.com/epp/idnLang-1.0"
 xmlns="http://www.w3.org/2001/XMLSchema"
 elementFormDefault="qualified">

<annotation>
  <documentation>
   Extensible Provisioning Protocol v1.0 domain name
   extension schema for IDN Lang Tag.
  </documentation>
</annotation>

<!--
Child elements found in EPP commands.
-->
  <element name="tag" type="language"/>

  <!--
 End of schema.
 -->
</schema>
```

XML templates/schema for rgp-poll-1.0

- Template: The templates for rgp-poll-1.0 can be found in Chapter 3, EPP Command Mapping of the relevant EPP documentation, http://www.verisigninc.com/assets/rgp-poll-mapping.pdf.
- Schema: This schema describes the extension mapping for poll notifications. The mapping extends the EPP base mapping to provide additional features for registry grace period (RGP) poll notifications.

```
<?xml version="1.0" encoding="UTF-8"?>

<schema targetNamespace="http://www.Verisign.com/epp/rgp-poll-1.0"
 xmlns:rgp-poll="http://www.Verisign.com/epp/rgp-poll-1.0"
 xmlns:eppcom="urn:ietf:params:xml:ns:eppcom-1.0"
 xmlns:rgp="urn:ietf:params:xml:ns:rgp-1.0"
 xmlns="http://www.w3.org/2001/XMLSchema"
 elementFormDefault="qualified">

<!--
Import common element types.
-->
<import namespace="urn:ietf:params:xml:ns:eppcom-1.0"
 schemaLocation="eppcom-1.0.xsd"/>
<import namespace="urn:ietf:params:xml:ns:rgp-1.0"
 schemaLocation="rgp-1.0.xsd"/>

<annotation>
  <documentation>
   Extensible Provisioning Protocol v1.0
   Verisign poll notification specification for registry grace period
   poll notifications.
  </documentation>
</annotation>

<!--
Child elements found in EPP commands.
-->
<element name="pollData" type="rgp-poll:pollDataType"/>

<!--
Child elements of the <notifyData> element for the
redemption grace period.
-->
<complexType name="pollDataType">
  <sequence>
    <element name="name" type="eppcom:labelType"/>
    <element name="rgpStatus" type="rgp:statusType"/>
    <element name="reqDate" type="dateTime"/>
    <element name="reportDueDate" type="dateTime"/>
  </sequence>
</complexType>
<
!--
End of schema.
-->
</schema>

XML templates/schema for whoisInf-1.0
•       Template: The templates for whoisInf-1.0 can be found in Chapter 3, EPP
Command Mapping of the relevant EPP documentation,
http://www.verisigninc.com/assets/whois-info-extension.pdf.
•       Schema: This schema describes the extension mapping for the Whois Info
extension. The mapping extends the EPP domain name mapping to provide additional
features for returning additional information needed for transfers.

<?xml version="1.0" encoding="UTF-8"?>

<schema targetNamespace="http://www.Verisign.com/epp/whoisInf-1.0"
 xmlns:whoisInf="http://www.Verisign.com/epp/whoisInf-1.0"
 xmlns:eppcom="urn:ietf:params:xml:ns:eppcom-1.0"
```

```
  xmlns="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified">

 <import namespace="urn:ietf:params:xml:ns:eppcom-1.0"
  schemaLocation="eppcom-1.0.xsd"/>

 <annotation>
  <documentation>
    Extensible Provisioning Protocol v1.0
    extension schema for Whois Info
  </documentation>
 </annotation>

 <!--
Possible Whois Info extension root elements.
-->
 <element name="whoisInf" type="whoisInf:whoisInfType"/>
 <element name="whoisInfData" type="whoisInf:whoisInfDataType"/>

 <!--
Child elements for the <whoisInf> extension which
is used as an extension to an info command.
-->
 <complexType name="whoisInfType">
   <sequence>
     <element name="flag" type="boolean"/>
   </sequence>
 </complexType>

 <!--
Child elements for the <whoisInfData> extension which
is used as an extension to the info response.
-->
 <complexType name="whoisInfDataType">
   <sequence>
   <element name="registrar" type="string"/>
   <element name="whoisServer" type="eppcom:labelType"
    minOccurs="0"/>
   <element name="url" type="token" minOccurs="0"/>
   <element name="irisServer" type="eppcom:labelType"
    minOccurs="0"/>
   </sequence>
   </complexType>

 </schema>
```

XML templates/schema for sync-1.0 (consoliDate)

- Template: The templates for sync-1.0 can be found in Chapter 3, EPP Command Mapping of the relevant EPP documentation, http://www.verisigninc.com/assets/consolidate-mapping.txt.
- Schema: This schema describes the extension mapping for the synchronization of domain name registration period expiration dates. This service is known as "ConsoliDate." The mapping extends the EPP domain name mapping to provide features that allow a protocol client to end a domain name registration period on a specific month and day.

```
  <?xml version="1.0" encoding="UTF-8"?>

    <schema targetNamespace="http://www.Verisign.com/epp/sync-1.0"
            xmlns:sync="http://www.Verisign.com/epp/sync-1.0"
            xmlns="http://www.w3.org/2001/XMLSchema"
```

```
            elementFormDefault="qualified">

      <annotation>
        <documentation>
         Extensible Provisioning Protocol v1.0 domain name
         extension schema for expiration date synchronization.
        </documentation>
      </annotation>

     <!--
    Child elements found in EPP commands.
    -->
      <element name="update" type="sync:updateType"/>

     <!--
    Child elements of the <update> command.
    -->
      <complexType name="updateType">
        <sequence>
          <element name="expMonthDay" type="gMonthDay"/>
        </sequence>
      </complexType>

     <!--
    End of schema.
    -->
     </schema>
```

XML templates/schema for namestoreExt-1.1

- Template: The templates for namestoreExt-1.1 can be found in Chapter 3, EPP Command Mapping of the relevant EPP documentation, http://www.verisigninc.com/assets/namestore-extension.pdf.
- Schema: This schema describes the extension mapping for the routing with an EPP intelligent gateway to a pluggable set of backend products and services. The mapping extends the EPP domain name and host mapping to provide a sub-product identifier to identify the target sub-product that the EPP operation is intended for.

```
<?xml version="1.0" encoding="UTF-8"?>

<schema targetNamespace="http://www.Verisign-grs.com/epp/namestoreExt-1.1"
 xmlns="http://www.w3.org/2001/XMLSchema"
 xmlns:namestoreExt="http://www.Verisign-grs.com/epp/namestoreExt-1.1"
 elementFormDefault="qualified">

<annotation>
  <documentation>
   Extensible Provisioning Protocol v1.0 Namestore extension schema
   for destination registry routing.
  </documentation>
</annotation>

<!-- General Data types. -->
<simpleType name="subProductType">
  <restriction base="token">
    <minLength value="1"/>
    <maxLength value="64"/>
  </restriction>
</simpleType>

<complexType name="extAnyType">
```

```
  (sequence)
    (any namespace="##other" maxOccurs="unbounded"/)
  (/sequence)
(/complexType)

(!-- Child elements found in EPP commands and responses. --)
(element name="namestoreExt" type="namestoreExt:namestoreExtType"/)

(!-- Child elements of the (product) command. --)
(complexType name="namestoreExtType")
  (sequence)
    (element name="subProduct"
     type="namestoreExt:subProductType"/)
  (/sequence)
(/complexType)

(!-- Child response elements. --)
(element name="nsExtErrData" type="namestoreExt:nsExtErrDataType"/)

(!-- (prdErrData) error response elements. --)
(complexType name="nsExtErrDataType")
  (sequence)
    (element name="msg" type="namestoreExt:msgType"/)
  (/sequence)
  (/complexType)

(!-- (prdErrData) (msg) element. --)
(complexType name="msgType")
  (simpleContent)
    (extension base="normalizedString")
      (attribute name="code"
       type="namestoreExt:prdErrCodeType" use="required"/)
      (attribute name="lang" type="language" default="en"/)
    (/extension)
  (/simpleContent)
(/complexType)

(!-- (prdErrData) error response codes. --)
(simpleType name="prdErrCodeType")
  (restriction base="unsignedShort")
    (enumeration value="1"/)
  (/restriction)
(/simpleType)

(!-- End of schema. --)
(/schema)
```

XML templates/schema for lowbalance-poll-1.0

- Template: The templates for lowbalance-poll-1.0 can be found in Chapter 3, EPP Command Mapping of the relevant EPP documentation, http://www.verisigninc.com/assets/low-balance-mapping.pdf.
- Schema: This schema describes the extension mapping for the account low balance notification. The mapping extends the EPP base mapping so an account holder can be notified via EPP poll messages whenever the available credit for an account reaches or goes below the credit threshold.

```
(?xml version="1.0" encoding="UTF-8"?)

(schema targetNamespace="http://www.Verisign.com/epp/lowbalance-poll-1.0"
 xmlns:lowbalance-poll="http://www.Verisign.com/epp/lowbalance-poll-1.0"
 xmlns:eppcom="urn:ietf:params:xml:ns:eppcom-1.0"
```

```
 xmlns="http://www.w3.org/2001/XMLSchema"
 elementFormDefault="qualified")

<!-- Import common element types.-->
<import namespace="urn:ietf:params:xml:ns:eppcom-1.0"
 schemaLocation="eppcom-1.0.xsd"/>

<annotation>
  <documentation>
   Extensible Provisioning Protocol v1.0
   Verisign poll notification specification for low balance notifications.
  </documentation>
</annotation>

<!--Child elements found in EPP commands.-->
<element name="pollData" type="lowbalance-poll:pollDataType"/>

<!--Child elements of the <notifyData> element for the low balance.-->
<complexType name="pollDataType">
  <sequence>
    <element name="registrarName" type="eppcom:labelType"/>
    <element name="creditLimit" type="normalizedString"/>
    <element name="creditThreshold"
     type="lowbalance-poll:thresholdType"/>
    <element name="availableCredit" type="normalizedString"/>
  </sequence>
</complexType>

<complexType name="thresholdType">
  <simpleContent>
    <extension base="normalizedString">
      <attribute name="type"
       type="lowbalance-poll:thresholdValueType"
       use="required"/>
    </extension>
  </simpleContent>
</complexType>

<simpleType name="thresholdValueType">
  <restriction base="token">
    <enumeration value="FIXED"/>
    <enumeration value="PERCENT"/>
  </restriction>
</simpleType>

<!-- End of schema.-->
</schema>
```

6 PROPRIETARY EPP EXTENSION CONSISTENCY WITH REGISTRATION LIFECYCLE

The Applicant's selected backend registry services provider's (Verisign's) proprietary EPP extensions, defined in Section 5 above, are consistent with the registration lifecycle documented in the response to Question 27, Registration Lifecycle. Details of the registration lifecycle are presented in that response. As new registry features are required, Verisign develops proprietary EPP extensions to address new operational requirements. Consistent with ICANN procedures Verisign adheres to all applicable Registry Services Evaluation Process (RSEP) procedures.

26. Whois

1 COMPLETE KNOWLEDGE AND UNDERSTANDING OF THIS ASPECT OF REGISTRY TECHNICAL REQUIREMENTS

Verisign, the Applicant's selected backend registry services provider, has operated the Whois lookup service for the gTLDs and ccTLDs it manages since 1991, and will provide these proven services for the TLD registry. In addition, it continues to work with the Internet community to improve the utility of Whois data, while thwarting its application for abusive uses.

1.1 High-Level Whois System Description

Like all other components of the Applicant's selected backend registry services provider's (Verisign's) registry service, Verisign's Whois system is designed and built for both reliability and performance in full compliance with applicable RFCs. Verisign's current Whois implementation has answered more than five billion Whois queries per month for the TLDs it manages, and has experienced more than 250,000 queries per minute in peak conditions. The proposed gTLD uses a Whois system design and approach that is comparable to the current implementation. Independent quality control testing ensures Verisign's Whois service is RFC-compliant through all phases of its lifecycle.

Verisign's redundant Whois databases further contribute to overall system availability and reliability. The hardware and software for its Whois service is architected to scale both horizontally (by adding more servers) and vertically (by adding more CPUs and memory to existing servers) to meet future need.

Verisign can fine-tune access to its Whois database on an individual Internet Protocol (IP) address basis, and it works with registrars to help ensure their services are not limited by any restriction placed on Whois. Verisign provides near real-time updates for Whois services for the TLDs under its management. As information is updated in the registration database, it is propagated to the Whois servers for quick publication. These updates align with the near real-time publication of Domain Name System (DNS) information as it is updated in the registration database. This capability is important for the TLD registry as it is Verisign's experience that when DNS data is updated in near real time, so should Whois data be updated to reflect the registration specifics of those domain names. Verisign's Whois response time has been less than 500 milliseconds for 95 percent of all Whois queries in .com, .net, .tv, and .cc. The response time in these TLDs, combined with Verisign's capacity, enables the Whois system to respond to up to 30,000 searches (or queries) per second for a total capacity of 2.6 billion queries per day.

The Whois software written by Verisign complies with RFC 3912. Verisign uses an advanced in-memory database technology to provide exceptional overall system performance and security. In accordance with RFC 3912, Verisign provides a website at whois.nic. (TLD) that provides free public query-based access to the registration data.

Verisign currently operates both thin and thick Whois systems.

Verisign commits to implementing a RESTful Whois service upon finalization of agreements with the IETF (Internet Engineering Task Force).

Provided Functionalities for User Interface

To use the Whois service via port 43, the user enters the applicable parameter on the command line as illustrated here:

- For domain name: whois EXAMPLE.TLD
- For registrar: whois "registrar Example Registrar, Inc."
- For name server: whois "NS1.EXAMPLE.TLD" or whois "name server (IP address)
"

To use the Whois service via the web-based directory service search interface:

- Go to http://whois.nic. (TLD)
- Click on the appropriate button (Domain, Registrar, or Name Server)
- Enter the applicable parameter:
  - Domain name, including the TLD (e.g., EXAMPLE.TLD)
  - Full name of the registrar, including punctuation (e.g., Example Registrar, Inc.)
  - Full host name or the IP address (e.g., NS1.EXAMPLE.TLD or 198.41.3.39)
- Click on the Submit button.

Provisions to Ensure That Access Is Limited to Legitimate Authorized Users and Is in Compliance with Applicable Privacy Laws or Policies
To further promote reliable and secure Whois operations, Verisign, the Applicant's selected backend registry services provider, has implemented rate-limiting characteristics within the Whois service software. For example, to prevent data mining or other abusive behavior, the service can throttle a specific requestor if the query rate exceeds a configurable threshold. In addition, QoS technology enables rate limiting of queries before they reach the servers, which helps protect against denial of service (DoS) and distributed denial of service (DDoS) attacks. Verisign's software also permits restrictions on search capabilities. For example, wild card searches can be disabled. If needed, it is possible to temporarily restrict and/or block requests coming from specific IP addresses for a configurable amount of time. Additional features that are configurable in the Whois software include help files, headers and footers for Whois query responses, statistics, and methods to memory map the database. Furthermore, Verisign is European Union (EU) Safe Harbor certified and has worked with European data protection authorities to address applicable privacy laws by developing a tiered Whois access structure that requires users who require access to more extensive data to (i) identify themselves, (ii) confirm that their use is for a specified purpose and (iii) enter into an agreement governing their use of the more extensive Whois data.

1.2 Relevant Network Diagrams

Figure 26 1 provides a summary network diagram of the Whois service provided by Verisign, the Applicant's selected backend registry services provider. The figure details the configuration with one resolution/Whois site. For this TLD Verisign provides Whois service from 6 of its 17 primary sites based on the proposed gTLD's traffic volume and patterns. A functionally equivalent resolution architecture configuration exists at each Whois site.

1.3 IT and Infrastructure Resources

Figure 26 2 summarizes the IT and infrastructure resources that Verisign, the Applicant's selected backend registry services provider, uses to provision Whois services from Verisign primary resolution sites. As needed, virtual machines are created based on actual and projected demand.

1.4 Description of Interconnectivity with Other Registry Systems

Figure 26 3 provides a technical overview of the registry system provided by Verisign, the Applicant's selected backend registry services provider, and shows how the Whois service component fits into this larger system and interconnects with other system components.

1.5 Frequency of Synchronization Between Servers

Synchronization between the SRS and the geographically distributed Whois resolution sites occurs approximately every three minutes. Verisign, the Applicant's selected backend registry services provider, uses a two-part Whois update process to ensure Whois data is accurate and available. Every 12 hours an initial file is distributed to each resolution site. This file is a complete copy of all Whois data fields associated with each domain name under management. As interactions with the SRS cause the Whois data to be changed, these incremental changes are distributed to the resolution sites as an incremental file update. This incremental update occurs approximately every three minutes. When the new 12-hour full update is distributed, this file includes all past incremental updates. Verisign's approach to frequency of synchronization between servers meets the Performance Specifications defined in Specification 10 of the Registry Agreement for new gTLDs.

2 TECHNICAL PLAN SCOPE/SCALE CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

Verisign, the Applicant's selected backend registry services provider, is an experienced backend registry provider that has developed and uses proprietary system scaling models to guide the growth of its TLD supporting infrastructure. These models direct Verisign's infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. Verisign periodically updates these models to account for the adoption of more capable and cost-effective technologies.

Verisign's scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the TLD with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its scaling models, Verisign derived the necessary infrastructure required to implement and sustain this gTLD. Verisign's pricing for the backend registry services it provides to the Applicant fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

3 TECHNICAL PLAN THAT IS ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

Verisign, the Applicant's selected backend registry services provider, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services it provides to the Applicant fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign's quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign's ability to align personnel resource growth to the scale increases of Verisign's TLD service offerings.

Verisign projects it will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support Whois services:

- Application Engineers: 19
- Database Engineers: 3
- Quality Assurance Engineers: 11

To implement and manage the TLD as described in this application, Verisign, the Applicant's selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.

When usage projections indicate a need for additional staff, Verisign's internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only this proposed gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

4 COMPLIANCE WITH RELEVANT RFC

The Applicant's selected backend registry services provider's (Verisign's) Whois

service complies with the data formats defined in Specification 4 of the Registry Agreement. Verisign will provision Whois services for registered domain names and associated data in the top-level domain (TLD). Verisign's Whois services are accessible over Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6), via both Transmission Control Protocol (TCP) port 43 and a web-based directory service at whois.nic. (TLD) , which in accordance with RFC 3912, provides free public query-based access to domain name, registrar, and name server lookups. Verisign's proposed Whois system meets all requirements as defined by ICANN for each registry under Verisign management. Evidence of this successful implementation, and thus compliance with the applicable RFCs, can be verified by a review of the .com and .net Registry Operator's Monthly Reports that Verisign files with ICANN. These reports provide evidence of Verisign's ability to meet registry operation service level agreements (SLAs) comparable to those detailed in Specification 10. The reports are accessible at the following URL: http://www.icann.org/en/tlds/monthly-reports/.

5 COMPLIANCE WITH SPECIFICATIONS 4 AND 10 OF REGISTRY AGREEMENT

In accordance with Specification 4, Verisign, the Applicant's selected backend registry services provider, provides a Whois service that is available via both port 43 in accordance with RFC 3912, and a web-based directory service at whois.nic. (TLD) also in accordance with RFC 3912, thereby providing free public query-based access. Verisign acknowledges that ICANN reserves the right to specify alternative formats and protocols, and upon such specification, Verisign will implement such alternative specification as soon as reasonably practicable.

The format of the following data fields conforms to the mappings specified in Extensible Provisioning Protocol (EPP) RFCs 5730 - 5734 so the display of this information (or values returned in Whois responses) can be uniformly processed and understood: domain name status, individual and organizational names, address, street, city, state/province, postal code, country, telephone and fax numbers, email addresses, date, and times.

Specifications for data objects, bulk access, and lookups comply with Specification 4 and are detailed in the following subsections, provided in both bulk access and lookup modes.

Bulk Access Mode. This data is provided on a daily schedule to a party designated from time to time in writing by ICANN. The specification of the content and format of this data, and the procedures for providing access, shall be as stated below, until revised in the ICANN Registry Agreement.

The data is provided in three files:

- Domain Name File: For each domain name, the file provides the domain name, server name for each name server, registrar ID, and updated date.
- Name Server File: For each registered name server, the file provides the server name, each IP address, registrar ID, and updated date.
- Registrar File: For each registrar, the following data elements are provided: registrar ID, registrar address, registrar telephone number, registrar email address, Whois server, referral URL, updated date, and the name, telephone number, and email address of all the registrar's administrative, billing, and technical contacts.

Lookup Mode. Figures 26 4 through Figure 26 6 provide the query and response format for domain name, registrar, and name server data objects.

5.1 Specification 10, RDDS Registry Performance Specifications

The Whois service meets all registration data directory services (RDDS) registry performance specifications detailed in Specification 10, Section 2. Evidence of this performance can be verified by a review of the .com and .net Registry Operator's Monthly Reports that Verisign files monthly with ICANN. These reports are accessible from the ICANN website at the following URL: http://www.icann.org/en/tlds/monthly-reports/.

In accordance with RDDS registry performance specifications detailed in Specification 10, Verisign's Whois service meets the following proven performance attributes:

- RDDS availability: 864 min of downtime (98%)

- RDDS query RTT: 2000 ms, for at least 95% of the queries
- RDDS update time: 60 min, for at least 95% of the probes

6 SEARCHABLE WHOIS

Verisign, the Applicant's selected backend registry services provider, provides a searchable Whois service for the TLD. Verisign has experience in providing tiered access to Whois for the .name registry, and uses these methods and control structures to help reduce potential malicious use of the function. The searchable Whois system currently uses Apache's Lucene full text search engine to index relevant Whois content with near-real time incremental updates from the provisioning system.

Features of the Verisign searchable Whois function include:

- Provision of a web-based searchable directory service
- Ability to perform partial match, at least, for the following data fields: domain name, contacts and registrant's name, and contact and registrant's postal address, including all the sub-fields described in EPP (e.g., street, city, state, or province)
- Ability to perform exact match, at least, on the following fields: registrar ID, name server name, and name server's IP address (only applies to IP addresses stored by the registry, i.e., glue records)
- Ability to perform Boolean search supporting, at least, the following logical operators to join a set of search criteria: AND, OR, NOT
- Search results that include domain names that match the selected search criteria

Verisign's implementation of searchable Whois is EU Safe Harbor certified and includes appropriate access control measures that help ensure that only legitimate authorized users can use the service. Furthermore, Verisign's compliance office monitors current ICANN policy and applicable privacy laws or policies to help ensure the solution is maintained within compliance of applicable regulations.

Features of these access control measures include:

- All unauthenticated searches are returned as thin results.
- Registry system authentication is used to grant access to appropriate users for thick Whois data search results.
- Account access is granted by the Applicant's defined TLD admin user.

Potential Forms of Abuse and Related Risk Mitigation. Leveraging its experience providing tiered access to Whois for the .name registry and interacting with ICANN, data protection authorities, and applicable industry groups, Verisign, the Applicant's selected backend registry services provider, is knowledgeable of the likely data mining forms of abuse associated with a searchable Whois service. Figure 26 7 summarizes these potential forms of abuse and Verisign's approach to mitigate the identified risk.

27. Registration Life Cycle

1 COMPLETE KNOWLEDGE AND UNDERSTANDING OF REGISTRATION LIFECYCLES AND STATES

Starting with domain name registration and continuing through domain name delete operations, the Applicant's selected backend registry services provider's (Verisign's) registry implements the full registration lifecycle for domain names supporting the operations in the Extensible Provisioning Protocol (EPP) specification. The registration lifecycle of the domain name starts with registration and traverses various states as specified in the following sections. The registry system provides options to update domain names with different server and client status codes that block operations based on the EPP specification. The system also provides different grace periods for different billable operations, where the price of the billable operation is credited back to the registrar if the

billable operation is removed within the grace period. Together Figure 27 1 and Figure 27 2 define the registration states comprising the registration lifecycle and explain the trigger points that cause state-to-state transitions. States are represented as green rectangles within Figure 27 1.

1.1 Registration Lifecycle of Create/Update/Delete

The following section details the create/update/delete processes and the related renewal process that Verisign, the Applicant's selected backend registry services provider, follows. For each process, this response defines the process function and its characterization, and as appropriate provides a process flow chart.

Create Process. The domain name lifecycle begins with a registration or what is referred to as a Domain Name Create operation in EPP. The system fully supports the EPP Domain Name Mapping as defined by RFC 5731, where the associated objects (e.g., hosts and contacts) are created independent of the domain name.

Process Characterization. The Domain Name Create command is received, validated, run through a set of business rules, persisted to the database, and committed in the database if all business rules pass. The domain name is included with the data flow to the DNS and Whois resolution services. If no name servers are supplied, the domain name is not included with the data flow to the DNS. A successfully created domain name has the created date and expiration date set in the database. Creates are subject to grace periods as described in Section 1.3 of this response, Add Grace Period, Redemption Grace Period, and Notice Periods for Renewals or Transfers.

The Domain Name Create operation is detailed in Figure 27 3 and requires the following attributes:

- A domain name that meets the string restrictions.
- A domain name that does not already exist.
- The registrar is authorized to create a domain name in the TLD.
- The registrar has available credit.
- A valid Authorization Information (Auth-Info) value.
- Required contacts (e.g., registrant, administrative contact, technical contact, and billing contact) are specified and exist.
- The specified name servers (hosts) exist, and there is a maximum of 13 name servers.
- A period in units of years with a maximum value of 10 (default period is one year).

Renewal Process. The domain name can be renewed unless it has any form of Pending Delete, Pending Transfer, or Renew Prohibited.

A request for renewal that sets the expiry date to more than ten years in the future is denied. The registrar must pass the current expiration date (without the timestamp) to support the idempotent features of EPP, where sending the same command a second time does not cause unexpected side effects.

Automatic renewal occurs when a domain name expires. On the expiration date, the registry extends the registration period one year and debits the registrar account balance. In the case of an auto-renewal of the domain name, a separate Auto-Renew grace period applies. Renewals are subject to grace periods as described in Section 1.3 of this response, Add Grace Period, Redemption Grace Period, and Notice Periods for Renewals or Transfers.

Process Characterization. The Domain Name Renew command is received, validated, authorized, and run through a set of business rules. The data is updated and committed in the database if it passes all business rules. The updated domain name's expiration date is included in the flow to the Whois resolution service.

The Domain Name Renew operation is detailed in Figure 27 4 and requires the following attributes:

- A domain name that exists and is sponsored by the requesting registrar.
- The registrar is authorized to renew a domain name in the TLD.
- The registrar has available credit.
- The passed current expiration date matches the domain name's expiration date.
- A period in units of years with a maximum value of 10 (default period is one year). A domain name expiry past ten years is not allowed.

Registrar Transfer Procedures. A registrant may transfer his/her domain name from his/her current registrar to another registrar. The database system allows a transfer as long as the transfer is not within the initial 60 days, per industry standard, of the original registration date.
The registrar transfer process goes through many process states, which are described in detail below, unless it has any form of Pending Delete, Pending Transfer, or Transfer Prohibited.
A transfer can only be initiated when the appropriate Auth-Info is supplied. The Auth-Info for transfer is only available to the current registrar. Any other registrar requesting to initiate a transfer on behalf of a registrant must obtain the Auth-Info from the registrant.
The Auth-Info is made available to the registrant upon request. The registrant is the only party other than the current registrar that has access to the Auth-Info.
Registrar transfer entails a specified extension of the expiry date for the object. The registrar transfer is a billable operation and is charged identically to a renewal for the same extension of the period. This period can be from one to ten years, in one-year increments.
Because registrar transfer involves an extension of the registration period, the rules and policies applying to how the resulting expiry date is set after transfer are based on the renewal policies on extension.
Per industry standard, a domain name cannot be transferred to another registrar within the first 60 days after registration. This restriction continues to apply if the domain name is renewed during the first 60 days. Transfer of the domain name changes the sponsoring registrar of the domain name, and also changes the child hosts (ns1.sample.xyz) of the domain name (sample .xyz).
The domain name transfer consists of five separate operations:

- Transfer Request (Figure 27 5): Executed by a non-sponsoring registrar with the valid Auth-Info provided by the registrant. The Transfer Request holds funds of the requesting registrar but does not bill the registrar until the transfer is completed. The sponsoring registrar receives a Transfer Request poll message.
- Transfer Cancel (Figure 27 6): Executed by the requesting registrar to cancel the pending transfer. The held funds of the requesting registrar are reversed. The sponsoring registrar receives a Transfer Cancel poll message.
- Transfer Approve (Figure 27 7): Executed by the sponsoring registrar to approve the Transfer Request. The requesting registrar is billed for the Transfer Request and the sponsoring registrar is credited for an applicable Auto-Renew grace period. The requesting registrar receives a Transfer Approve poll message.
- Transfer Reject (Figure 27 8): Executed by the sponsoring registrar to reject the pending transfer. The held funds of the requesting registrar are reversed. The requesting registrar receives a Transfer Reject poll message.
- Transfer Query (Figure 27 9): Executed by either the requesting registrar or the sponsoring registrar of the last transfer.

The registry auto-approves a transfer if the sponsoring registrar takes no action. The requesting registrar is billed for the Transfer Request and the sponsoring registrar is credited for an applicable Auto-Renew grace period. The requesting registrar and the sponsoring registrar receive a Transfer Auto-Approve poll message.
Delete Process. A registrar may choose to delete the domain name at any time.
Process Characterization. The domain name can be deleted, unless it has any form of Pending Delete, Pending Transfer, or Delete Prohibited.
A domain name is also prohibited from deletion if it has any in-zone child hosts that are name servers for domain names. For example, the domain name "sample.xyz" cannot be deleted if an in-zone host "ns.sample.xyz" exists and is a name server for "sample2.xyz."
If the Domain Name Delete occurs within the Add grace period, the domain name is immediately deleted and the sponsoring registrar is credited for the Domain Name Create. If the Domain Name Delete occurs outside the Add grace period, it follows the Redemption grace period (RGP) lifecycle.
Update Process. The sponsoring registrar can update the following attributes of a

domain name:
- Auth-Info
- Name servers
- Contacts (i.e., registrant, administrative contact, technical contact, and billing contact)
- Statuses (e.g., Client Delete Prohibited, Client Hold, Client Renew Prohibited, Client Transfer Prohibited, Client Update Prohibited)

Process Characterization. Updates are allowed provided that the update includes the removal of any Update Prohibited status. The Domain Name Update operation is detailed in Figure 27 10.
A domain name can be updated unless it has any form of Pending Delete, Pending Transfer, or Update Prohibited.

1.2 Pending, Locked, Expired, and Transferred
Verisign, the Applicant's selected backend registry services provider, handles pending, locked, expired, and transferred domain names as described here. When the domain name is deleted after the five-day Add grace period, it enters into the Pending Delete state. The registrant can return its domain name to active any time within the five-day Pending Delete grace period. After the five-day Pending Delete grace period expires, the domain name enters the Redemption Pending state and then is deleted by the system. The registrant can restore the domain name at any time during the Redemption Pending state.
When a non-sponsoring registrar initiates the domain name transfer request, the domain name enters Pending Transfer state and a notification is mailed to the sponsoring registrar for approvals. If the sponsoring registrar doesn't respond within five days, the Pending Transfer expires and the transfer request is automatically approved.
EPP specifies both client (registrar) and server (registry) status codes that can be used to prevent registry changes that are not intended by the registrant. Currently, many registrars use the client status codes to protect against inadvertent modifications that would affect their customers' high-profile or valuable domain names.
Verisign's registry service supports the following client (registrar) and server (registry) status codes:
- clientHold
- clientRenewProhibited
- clientTransferProhibited
- clientUpdateProhibited
- clientDeleteProhibited
- serverHold
- serverRenewProhibited
- serverTransferProhibited
- serverUpdateProhibited
- serverDeleteProhibited

1.3 Add Grace Period, Redemption Grace Period, and Notice Periods for Renewals or Transfers
Verisign, the Applicant's selected backend registry services provider, handles Add grace periods, Redemption grace periods, and notice periods for renewals or transfers as described here.
- Add Grace Period: The Add grace period is a specified number of days following the initial registration of the domain name. The current value of the Add grace period for all registrars is five days.
- Redemption Grace Period: If the domain name is deleted after the five-day grace period expires, it enters the Redemption grace period and then is deleted by the system. The registrant has an option to use the Restore Request command to restore the domain name within the Redemption grace period. In this scenario, the domain name goes to Pending Restore state if there is a Restore Request command within 30 days of the Redemption grace period. From the Pending Restore state, it goes either to the OK state, if there is a Restore Report Submission command within seven days of the Restore Request grace period, or a Redemption Period state if

there is no Restore Report Submission command within seven days of the Restore Request grace period.
• Renew Grace Period: The Renew/Extend grace period is a specified number of days following the renewal/extension of the domain name's registration period. The current value of the Renew/Extend grace period is five days.
• Auto-Renew Grace Period: All auto-renewed domain names have a grace period of 45 days.
• Transfer Grace Period: Domain names have a five-day Transfer grace period.

1.4 Aspects of the Registration Lifecycle Not Covered by Standard EPP RFCs

The Applicant's selected backend registry services provider's (Verisign's) registration lifecycle processes and code implementations adhere to the standard EPP RFCs related to the registration lifecycle. By adhering to the RFCs, Verisign's registration lifecycle is complete and addresses each registration-related task comprising the lifecycle. No aspect of Verisign's registration lifecycle is not covered by one of the standard EPP RFCs and thus no additional definitions are provided in this response.

2 CONSISTENCY WITH ANY SPECIFIC COMMITMENTS MADE TO REGISTRANTS AS ADAPTED TO THE OVERALL BUSINESS APPROACH FOR THE PROPOSED gTLD

The registration lifecycle described above applies to this TLD as well as other TLDs managed by Verisign, the Applicant's selected backend registry services provider; thus Verisign remains consistent with commitments made to its registrants. No unique or specific registration lifecycle modifications or adaptations are required to support the overall business approach for the TLD. To accommodate a range of registries, Verisign's registry implementation is capable of offering both a thin and thick Whois implementation, which is also built upon Verisign's award-winning ATLAS infrastructure.

3 COMPLIANCE WITH RELEVANT RFCs

The Applicant's selected backend registry services provider's (Verisign's) registration lifecycle complies with applicable RFCs, specifically RFCs 5730 - 5734 and 3915. The system fully supports the EPP Domain Name Mapping as defined by RFC 5731, where the associated objects (e.g., hosts and contacts) are created independent of the domain name.

In addition, in accordance with RFCs 5732 and 5733, the Verisign registration system enforces the following domain name registration constraints:
• Uniqueness/Multiplicity: A second-level domain name is unique in the TLD database. Two identical second-level domain names cannot simultaneously exist in the TLD. Further, a second-level domain name cannot be created if it conflicts with a reserved domain name.
• Point of Contact Associations: The domain name is associated with the following points of contact. Contacts are created and managed independently according to RFC 5733.
• Registrant
• Administrative contact
• Technical contact
• Billing contact
• Domain Name Associations: Each domain name is associated with:
• A maximum of 13 hosts, which are created and managed independently according to RFC 5732
• An Auth-Info, which is used to authorize certain operations on the object
• Status(es), which are used to describe the domain name's status in the registry
• A created date, updated date, and expiry date

4 DEMONSTRATES THAT TECHNICAL RESOURCES REQUIRED TO CARRY THROUGH THE PLANS FOR THIS ELEMENT ARE ALREADY ON HAND OR READILY AVAILABLE

Verisign, the Applicant's selected backend registry services provider, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to continually

right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services it provides to the Applicant fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.
Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign's quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign's ability to align personnel resource growth to the scale increases of Verisign's TLD service offerings.

Verisign projects it will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support the registration lifecycle:

- Application Engineers: 19
- Customer Support Personnel: 36
- Database Administrators: 8
- Database Engineers: 3
- Quality Assurance Engineers: 11
- SRS System Administrators: 13

To implement and manage the TLD as described in this application, Verisign, the Applicant's selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.
When usage projections indicate a need for additional staff, Verisign's internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only this proposed gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

28. Abuse Prevention and Mitigation

1. COMPREHENSIVE ABUSE POLICIES, WHICH INCLUDE CLEAR DEFINITIONS OF WHAT CONSTITUTES ABUSE IN THE TLD, AND PROCEDURES THAT WILL EFFECTIVELY MINIMIZE POTENTIAL FOR ABUSE IN THE TLD
Applicant intends to request from ICANN an exemption from Specification 9 of the ICANN-Registry Operator Registry Agreement. As such, Applicant intends to function in such a way that all domain name registrations in the TLD shall be registered to and maintained by Applicant and Applicant will not sell, distribute or transfer control of domain name registrations to any party that is not an Affiliate of Applicant as defined in the ICANN-Registry Operator Registry

Agreement. All domain name registrations intended to be used within Applicant's registry will be registered to and controlled and maintained by Applicant and for the benefit of Applicant and its users, parents, sisters and Affiliates.

In the event that Applicant is not granted an exemption from Specification 9, Applicant will partner with a corporate registrar with expertise in running a registry to support such efforts. Applicant intends to partner with its current corporate registrar or one of similar technical capability and expertise and allocate the appropriate funds and human resources to ensure that both itself, as the registry operator, and its selected registrar are at all times in compliance with ICANN guidelines.

Several measures for discouraging domain name abuse in the Applicant's TLD and the registration in the Applicant's TLD of domain names that infringe the intellectual property rights of others are detailed within this section, in the response to question #29 and throughout other portions of the application. Additionally, it is noted that a major concern of other TLDs, namely, trademark infringement, is of lesser concern as such relates to the Applicant's TLD. There will be little to no risk of domain name abuse and improper registration of any infringing subdomains or the like in the TLD and Applicant believes sufficient protection for famous names and trademarks will be provided for because of the fact that: (i) Applicant's TLD intends to function as a Specification 9 exempt TLD and, thus, all registrations will be approved by and registered only to Applicant; (ii) Applicant will implement and comply with all ICANN-mandated rights protection mechanisms (see response to question #29), and (iii) Applicant's current policies will prohibit any registrations by any party that is not the Applicant and registrations will be associated with Applicant and its users, parents, sisters and Affiliates, and more particularly, the content and branded material associated with those entities. For that reason, in any case, Applicant believes that there will be little to no likelihood of confusion between the trademark holder and Applicant. As users come to know Applicant's TLD, they will come to understand that any and all content associated with the TLD is also associated with Applicant and its users, parents, sisters and Affiliates, and no other party.

This means that there will be little pressure on current trademark holders to believe that they have to defensively obtain all of their trademarks within the TLD. One event in which a trademark right may be affected is the unlikely instance in which a commonly known name which is identical or confusingly similar to a trademark is registered. In this event, a trademark holder may submit a request to Applicant to remove the registration or cease use of the subdomain. Applicant is committed to making every attempt to resolve such disputes in a fair and equitable manner and demonstrating the high value Applicant places on intellectual property rights, including rights associated with trademarks. Alternatively, or in addition, the trademark holder is free to file a URS, UDRP or any other dispute resolution action pursuant to the ICANN-approved new gTLD guidelines. Applicant will comply with any and all decisions and orders issued by the adjudicating bodies of these dispute resolution authorities and procedures. In particular, protection for trademark holders will be provided, without limitation, during the implementation phase of the Trademark Clearinghouse in compliance with protection mechanisms related to the requirements of Specification 7 of the Registry Agreement, the Trademark Clearinghouse and any other relevant rights protections mechanisms.

Furthermore, Applicant will provide to ICANN in this application and publish on its website the abuse policy and contact details (as included below and including a valid email and mailing address) to be responsible or addressing matters requiring attention and to handle inquiries related to malicious conduct in the TLD in a timely manner.

Additionally, a reserved list of names will be employed to prevent inappropriate name registrations. This list may be updated periodically based on ICANN

directives and guidance. This list will include, among others, ICANN's list of reserved names in the Registry Agreement, and certain geographic identifiers as enumerated in the response to question #22. The list of names reserved from reservation is enumerated below:

- ICANN and IANA-related names (reserved at second and at all other levels)
  - aso
  - gnso
  - icann
  - internic
  - ccnso
  - afrinic
  - apnic
  - arin
  - example
  - gtld-servers
  - iab
  - iana
  - iana-servers
  - iesg
  - ietf
  - irtf
  - istf
  - lacnic
  - latnic
  - rfc-editor
  - ripe
  - root-servers
- Single-character and two-character labels (reserved at the second level)
- Tagged domains - labels with hyphens in the third and fourth character positions
- Registry operations names - (reserved at the second level) reserved for use in connection with the operation of the registry for the Registry TLD. Registry Operator may use them, but upon conclusion of Registry Operator's designation as operator of the registry for the Registry TLD they shall be transferred as specified by ICANN:
  - NIC
  - WHOIS
  - WWW
- TLD labels (e.g., aero, arpa, biz, com, etc.)
- Geographic and Geopolitical Names. All geographic and geopolitical names contained in the ISO 3166-1 list from time to time shall initially be reserved at both the second level and at all other levels within the TLD at which the Registry Operator provides for registrations. All names shall be reserved both in English and in all related official languages as may be directed by ICANN or the GAC.

  - In addition, Registry Operator shall reserve names of territories, distinct geographic locations, and other geographic and geopolitical names as ICANN may direct from time to time. Such names may be reserved from registration during any sunrise period, and may be registered in ICANN's name prior to start-up and open registration in the TLD. Registry Operator may post and maintain an updated listing of all such names on its website, which list may be subject to change at ICANN's direction. Upon determination by ICANN of appropriate standards and qualifications for registration following input from interested parties in the Internet community, such names may be approved for registration to the appropriate authoritative body.

The Applicant's TLD will comply with all applicable trademark and anti-cybersquatting legislation. In the event of an inconsistency between such legislation and the procedures of Applicant's TLD, Applicant will revise its procedures to be in compliance therewith.

Should Applicant function as a Specification 9 exempt Registry Operator, Applicant will restrict the transfer of registrations of domain names within its TLD to third parties.

1.1 Abuse Prevention and Mitigation Implementation Plan
In addition to developing ICANN policies and the Applicant policies as articulated above, below and pursuant to the attached Abuse Prevention and Mitigation Implementation Plan, the registration process will limit abusive registration practices commonly associated with TLDs in which abusive registrants use false contact information to evade identification or legal process. Applicant's TLD intends to function, per the ICANN-Registry Operator Registry Agreement, as a Specification 9 exempt TLD whereby all domain name registrations in the TLD shall be registered to and maintained by Applicant and Applicant will not sell, distribute or transfer control of domain name registrations to any party that is not an Affiliate of Applicant as defined in the ICANN-Registry Operator Registry Agreement. All domain name registrations intended to be used within Applicant's registry will be registered to and controlled and maintained by Applicant and its verified and authenticated Affiliates and for the benefit of Applicant and its users, parents, sisters and Affiliates. All registrations must be requested through one of Applicant's internal channels and must be verified and approved before registration. The verification process will be in operation on an ongoing basis. The verification process is designed to establish that a prospective registrant meets the registration criteria.
a. A variety of automated and manual procedures will be utilized for verification, including a cross-check of registration against information held by Applicant.
b. Eligibility of prospective registrants will be verified prior to the addition of a name to the Applicant's TLD zone file, including but not limited to, review of the request for registration by Applicant's compliance staff who will attempt to manually verify the affiliation of the prospective registrant with the Applicant.
c. Applicant will verify contact/WHOIS data for prospective registrants prior to the addition of a name to the Applicant's TLD zone file.
d. Applicant will maintain verified contact data for the actual registrant as well as for any proxy services utilized by registrant. Proxy services eligible for use are limited to services that have demonstrated responsible and responsive business services.
e. Prospective registrants must represent and warrant that neither the registration of the desired string, nor the manner in which the registration will be used, infringes the legal rights of third parties.
f. Prospective registrants will disclose their intended use for the domain. Registration will be refused to those who do not indicate at least one acceptable use of the domain. Acceptable uses of the TLD include, but are not limited to the bona fide use or bona fide intent to use the domain name or any content, software, materials, graphics or other information thereon to permit Internet users to access one or more host computers through the DNS:
- to exchange goods, services or property of any kind;
- in the ordinary course of trade or business; or
- to facilitate the exchange of goods, services, information, or property of any kind, or the ordinary course of trade or business.

Additionally, Applicant will implement a number of mechanisms pursuant to all ICANN guidelines and the Registry Agreement for those who are not affiliated with the Applicant to protect their intellectual property.
a. Pre-Reservation Service: Applicant may enable existing holders of a trademark to block Applicant's TLD registrations that correspond to their existing registrations in other ICANN recognized TLDs.
b. Trademark Clearinghouse: Trademark owners will have an extended period in which they can register their trademarks with the Trademark Clearinghouse. Once registration begins, if a registrant attempts to register a name that has been registered with the Trademark Clearinghouse, the prospective registrant will be

notified of the existence of the registration with the Trademark Clearinghouse.
Dispute Resolution Procedures: Registered domains will be subject to challenge under ordinary domain dispute procedures set forth by ICANN, including but not limited to, Uniform Domain-Name Dispute-Resolution Policy (UDRP), Uniform Rapid Suspension system (URS), Trademark Post-Delegation Dispute Procedure (PDDRP), and Registration Restriction Dispute Resolution Procedure (RRDRP). Applicant agrees to implement and adhere to any remedies imposed by decision makers under such procedures.

1.2 Policies for Handling Complaints Regarding Abuse

Applicant reserves the right to deny, cancel or transfer any registration or transaction, or place any domain name(s) on registry lock, hold or similar status, that it deems necessary, in its discretion; (1) to protect the integrity and stability of the registry; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of Applicant, as well as its Affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the Registration Agreement; or (5) to correct mistakes made by Applicant or its registrar in connection with a domain name registration.

During review of any complaint, Applicant will consider the standards set forth in the ICANN UDRP, in addition to the following modifications:

a. Evidence that a domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights can include evidence that the domain name is "...confusingly similar to a trademark, service mark or trade name in which the complainant has rights or the name under which the complainant does business...." This will grant standing to an entity based upon the entity's trade name or name under which it does business.

b. Evidence that a domain has been registered and is being used in bad faith will require a showing that the domain has been registered and/or is being used in bad faith. This will allow a claim based upon bad faith on the part of the registrant during either registration or use.

c. Additional indicia of bad faith use will be considered. These indicia will include (1) use of the domain name inconsistent with the Code, and (2) use of the domain name in connection with a list of prohibited uses, which will include pornography, hacks/cracks content, etc. The list of prohibited uses may be compiled by Applicant and outside advisors.

d. Enumerated circumstances for proving a right and legitimate interest will include trade names and names under which business is done where trademarks and service marks currently are noted. A showing of bad faith registration or use, however, will be considered as prima facie evidence of no legitimate interest.

Applicant also reserves the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute.

All reports of abuse should be sent to an email address that will be publicly identified by Applicant for receiving reports of abuse.

1.3 Proposed Measures for Removal of Orphan Glue Records

Although orphan glue records often support correct and ordinary operation of the Domain Name System (DNS), registry operators will be required to remove orphan glue records (as defined at http://www.icann.org/en/committees/security/sac048.pdf) when provided with evidence in written form that such records are present in connection with malicious conduct. Applicant's selected backend registry services provider's (Verisign's) registration system is specifically designed to not allow orphan glue records. Registrars are required to delete/move all dependent DNS records before they are allowed to delete the parent domain.

To prevent orphan glue records, Verisign performs the following checks before removing a domain or name server:

Checks during domain delete:

- Parent domain delete is not allowed if any other domain in the zone refers to the child name server.
- If the parent domain is the only domain using the child name server, then both the domain and the glue record are removed from the zone.

Check during explicit name server delete:
• Verisign confirms that the current name server is not referenced by any domain name (in-zone) before deleting the name server.

Zone-file impact:
• If the parent domain references the child name server AND if other domains in the zone also reference it AND if the parent domain name is assigned a serverHold status, then the parent domain goes out of the zone but the name server glue record does not.
• If no domains reference a name server, then the zone file removes the glue record.

1.4 Resourcing Plans
Details related to resourcing plans for the initial implementation and ongoing maintenance of the Applicant's abuse plan are provided in Section 2 of this response.
1.5 Measures to Promote WHOIS Accuracy
Applicant will maintain a shared registration system for Applicant's selected registrar. WHOIS access will be facilitated in compliance with ICANN policies, including without limitation the Registry Agreement. It is anticipated that information will be provided which is consistent with the WHOIS information currently provided in other TLDs, including identification of the registrant and contact information therefore, administrative, technical and billing contacts, creation and expiration date and DNS settings. One way that Applicant may ensure compliance with all applicable policies is to mandate that all requests for domains will be required to come from a verified internal corporate channel to ensure that the requestor is affiliated with Applicant. Such requests will be subject to an internal review and approval process that may be amended from time to time. In addition, Applicant may provide for additional measures, such as to conduct audits (e.g., compliance with requirements to make WHOIS available, and with the annual WHOIS Data Reminder Policy (WDRP)); investigate complaints of non-compliance (e.g., responses to WHOIS Data Problem Service (WDPRS) notifications); develop documented internal processes and training for personnel assigned by Applicant to complete WHOIS data to ensure that data is provided completely and accurately.

At this point, Applicant anticipates that registrant information will be protected or made available as required by ICANN, applicable law or other regulatory bodies. For technical details regarding how a complete, up-to-date, reliable and conveniently accessible WHOIS database will be provided, see response to question #26.

Applicant ensures that the WHOIS database and access thereto will comply with emerging ICANN privacy policies, if and when they become approved.
1.5.1 Authentication of Registrant Information
Applicant intends to function, per the ICANN-Registry Operator Registry Agreement, as a Specification 9 exempt TLD whereby all domain name registrations in the TLD shall be registered to and maintained by Applicant and Applicant will not sell, distribute or transfer control of domain name registrations to any party that is not an Affiliate of Applicant as defined in the ICANN-Registry Operator Registry Agreement. All domain name registrations intended to be used within Applicant's registry will be registered to and controlled and maintained by Applicant and for the benefit of Applicant and its users, parents, sisters and Affiliates. See also section 1.1 above.
1.5.2 Regular Monitoring of Registration Data for Accuracy and Completeness
Applicant intends to function, per the ICANN-Registry Operator Registry Agreement, as a Specification 9 exempt TLD whereby all domain name registrations in the TLD shall be registered to and maintained by Applicant and Applicant will not sell, distribute or transfer control of domain name registrations to any party that is not an Affiliate of Applicant as defined in the ICANN-Registry Operator Registry Agreement. All domain name registrations intended to be used within Applicant's registry will be registered to and controlled and maintained by Applicant and for

the benefit of Applicant and its users, parents, sisters and Affiliates. As the only registrations permitted will be from the Applicant entity, the monitoring of the accuracy of registration data will be reasonable and Applicant will periodically (on at least an annual basis) monitor the accuracy and completeness of such information. Verisign, Applicant's selected backend registry services provider, has established policies and procedures to encourage registrar compliance with ICANN's WHOIS accuracy requirements. Verisign provides the following services to Applicant for incorporation into its full-service registry operations. Verisign, the Applicant's selected backend registry services provider, has established policies and procedures to encourage registrar compliance with ICANN's WHOIS accuracy requirements. Verisign provides the following services to the Applicant for incorporation into its full-service registry operations. Registrar self-certification. Applicant intends to function, per the ICANN-Registry Operator Registry Agreement, as a Specification 9 exempt TLD whereby all domain name registrations in the TLD shall be registered to and maintained by Applicant and Applicant will not sell, distribute or transfer control of domain name registrations to any party that is not an Affiliate of Applicant as defined in the ICANN-Registry Operator Registry Agreement. All domain name registrations intended to be used within Applicant's registry will be registered to and controlled and maintained by Applicant and for the benefit of Applicant and its users, parents, sisters and Affiliates.

WHOIS data reminder process. Verisign regularly reminds registrars of their obligation to comply with ICANN's WHOIS Data Reminder Policy, which was adopted by ICANN as a consensus policy on 27 March 2003 (http://www.icann.org/en/registrars/wdrp.htm). Verisign sends a notice to all registrars once a year reminding them of their obligation to be diligent in validating the WHOIS information provided during the registration process, to investigate claims of fraudulent WHOIS information, and to cancel domain name registrations for which WHOIS information is determined to be invalid. Notwithstanding the above, Applicant intends to function, per the ICANN-Registry Operator Registry Agreement, as a Specification 9 exempt TLD whereby all domain name registrations in the TLD shall be registered to and maintained by Applicant and Applicant will not sell, distribute or transfer control of domain name registrations to any party that is not an Affiliate of Applicant as defined in the ICANN-Registry Operator Registry Agreement. All domain name registrations intended to be used within Applicant's registry will be registered to and controlled and maintained by Applicant and for the benefit of Applicant and its users, parents, sisters and Affiliates.

1.5.3 Use of Registrars

Applicant intends to function, per the ICANN-Registry Operator Registry Agreement, as a Specification 9 exempt TLD whereby all domain name registrations in the TLD shall be registered to and maintained by Applicant and Applicant will not sell, distribute or transfer control of domain name registrations to any party that is not an Affiliate of Applicant as defined in the ICANN-Registry Operator Registry Agreement. All domain name registrations intended to be used within Applicant's registry will be registered to and controlled and maintained by Applicant and for the benefit of Applicant and its users, parents, sisters and Affiliates.

At the appropriate time, between post-submission of this application and prior to the Applicant's TLD launch, Applicant will identify, determine and engage the proper service provider (e.g. Applicant-approved registrar and/or selected backend registry services provider, Verisign) to support its provision of registration and abuse policies. Any engagement for the implementation and provision of such services shall be in compliance with all ICANN-mandated regulations, agreements, guidance and policies, as it is of paramount importance of the Applicant to protect the rights of all rightsholders.

1.6 Malicious or Abusive Behavior Definitions, Metrics, and Service Level Requirements for Resolution

Pursuant to the attached Abuse Prevention and Mitigation Implementation Plan, Applicant shall implement the following anti-abuse policy as a guideline:

Applicant intends to function, per the ICANN-Registry Operator Registry Agreement, as a Specification 9 exempt TLD whereby all domain name registrations in the TLD shall be registered to and maintained by Applicant and Applicant will not sell, distribute or transfer control of domain name registrations to any party that is not an Affiliate of Applicant as defined in the ICANN-Registry Operator Registry Agreement. All domain name registrations intended to be used within Applicant's registry will be registered to and controlled and maintained by Applicant and for the benefit of Applicant and its users, parents, sisters and Affiliates. Access to domain functions will be limited to Applicant and its engaged service provider partners by implementing and complying with their established safeguards and access features as articulated below.

1.7.1 Multi-Factor Authentication

To ensure proper access to domain functions, the Applicant incorporates Verisign's Registry-Registrar Two-Factor Authentication Service into its full-service registry operations. The service is designed to improve domain name security and assist registrars in protecting the accounts they manage by providing another level of assurance that only authorized personnel can communicate with the registry. As part of the service, dynamic one-time passwords (OTPs) augment the user names and passwords currently used to process update, transfer, and/or deletion requests. These one-time passwords enable transaction processing to be based on requests that are validated both by "what users know" (i.e., their user name and password) and "what users have" (i.e., a two-factor authentication credential with a one-time-password).

Registrars can use the one-time-password when communicating directly with Verisign's Customer Service department as well as when using the registrar portal to make manual updates, transfers, and/or deletion transactions. The Two-Factor Authentication Service is an optional service offered to registrars that execute the Registry-Registrar Two-Factor Authentication Service Agreement. As shown in Figure 28-1, the registrars' authorized contacts use the OTP to enable strong authentication when they contact the registry. There is no charge for the Registry-Registrar Two-Factor Authentication Service. It is enabled only for registrars that wish to take advantage of the added security provided by the service.

1.7.2 Requiring Multiple, Unique Points of Contact

Unique points of contact (POC) and their respective actions will be determined by Applicant at the appropriate time prior to the implementation of the gTLD.

1.7.3 Requiring the Notification of Multiple, Unique Points of Contact

Unique points of contact (POC) and their respective actions will be determined by Applicant at the appropriate time prior to the implementation of the gTLD.

2. TECHNICAL PLAN THAT IS ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

Resource Planning

Applicant projects it will use the following personnel roles to support the implementation of the policies articulated in this section:

- 1 senior level executive
- 1 marketing/business manager
- 1 technical manager
- 1 administrative professional

To implement and manage Applicant's gTLD as described in this application, Applicant can scale as needed, and utilize resources provided by our parent company, as defined above. In particular, personnel currently involved in the operation of parent entity's existing .com business can assist with the needs of this new gTLD and may be transitioned over to supporting the gTLD as the .com businesses wind down in favor of the new gTLD. In addition to these individuals, Applicant parent entity will support implementation of these policies through the provision of their resources as well as additional outside resources on an as-needed basis. Support from our parent company will include access to a law department, finance department, information systems, technical support, human resources and such other administrative support that may be required. In particular, we anticipate using outside advisors and lawyers to assist in managing any disputes which must be resolved. Once the top level domain has been awarded,

we do not anticipate disputes beyond what is frequently encountered in operating the .com. However, given the expanded opportunities associated with operating the top level domain, we have increased the likelihood of disputes, take down notices or such other matters and increased the .com dispute resolution budget. We will utilize outside advisors to provide the additional talent and resources and specialized knowledge that we cannot cost effectively maintain internally. Projected costs associated with these resources are further discussed in the response to Question 47 below.

Resource Planning Specific to Backend Registry Activities

Verisign, the Applicant's selected backend registry services provider, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services it provides to the Applicant fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign's quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign's ability to align personnel resource growth to the scale increases of Verisign's TLD service offerings.

Verisign projects it will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support abuse prevention and mitigation:

- Application Engineers: 19
- Business Continuity Personnel: 3
- Customer Affairs Organization: 9
- Customer Support Personnel: 36
- Information Security Engineers: 11
- Network Administrators: 11
- Network Architects: 4
- Network Operations Center (NOC) Engineers: 33
- Project Managers: 25
- Quality Assurance Engineers: 11
- Systems Architects: 9

To implement and manage the TLD as described in this application, Verisign, the Applicant's selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.

When usage projections indicate a need for additional staff, Verisign's internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only this proposed gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams,

Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

3. POLICIES AND PROCEDURES IDENTIFY AND ADDRESS THE ABUSIVE USE OF REGISTERED NAMES AT START-UP AND ON AN ONGOING BASIS

3.1 Start-Up Anti-Abuse Policies and Procedures

a. Pre-Reservation Service: Applicant may enable existing holders of a trademark to block Applicant registrations that correspond to their existing registrations in other ICANN recognized TLDs.

b. Trademark Clearinghouse: Trademark owners will have an extended period in which they can register their trademarks with the Trademark Clearinghouse. Once registration begins, if a registrant attempts to register a name that has been registered with the Trademark Clearinghouse, the prospective registrant will be notified of the existence of the registration with the Trademark Clearinghouse.

3.2 Ongoing Anti-Abuse Policies and Procedures

3.2.1 Policies and Procedures That Identify Malicious or Abusive Behavior

Verisign, the Applicant's selected backend registry services provider, provides the following service to the Applicant for incorporation into its full-service registry operations.

Malware scanning service. Registrants are often unknowing victims of malware exploits. Verisign has developed proprietary code to help identify malware in the zones it manages, which in turn helps registrars by identifying malicious code hidden in their domain names.

Verisign's malware scanning service helps prevent websites from infecting other websites by scanning web pages for embedded malicious content that will infect visitors' websites. Verisign's malware scanning technology uses a combination of in-depth malware behavioral analysis, anti-virus results, detailed malware patterns, and network analysis to discover known exploits for the particular scanned zone. If malware is detected, the service sends the registrar a report that contains the number of malicious domains found and details about malicious content within its TLD zones. Reports with remediation instructions are provided to help registrars and registrants eliminate the identified malware from the registrant's website.

3.2.2 Policies and Procedures That Address the Abusive Use of Registered Names

Suspension processes. In addition to the safeguards and mechanisms additionally provided for above and below and those required by ICANN and applicable law, rightsholders will have the opportunity to provide written notification of claimed abuse and Applicant will investigate notices of abuse and take appropriate actions pursuant to the policies articulated herein and those required by ICANN and applicable law.

Dispute Resolution Procedures: Registered domains will be subject to challenge under ordinary domain dispute procedures set forth by ICANN, including but not limited to, Uniform Domain-Name Dispute-Resolution Policy (UDRP), Uniform Rapid Suspension system (URS), Trademark Post-Delegation Dispute Procedure (PDDRP), and Registration Restriction Dispute Resolution Procedure (RRDRP). Applicant agrees to implement and adhere to any remedies imposed by decision makers under such procedures.

Compliance with Court Orders and Law Enforcement Requests: Applicant reserves the right, but disclaims any obligation or responsibility, to (a) refuse to post or communicate or remove any submission from any Applicant site that is deemed to be abusive and (b) identify any user to third parties, and/or disclose to third parties any submission or personally identifiable information, when we believe in good faith that such identification or disclosure will either (i) facilitate compliance with laws, including, for example, compliance with a court order or subpoena, or (ii) help to enforce these policies and/or other Applicant rules or regulations, and/or protect the safety or security of any person or property, including any Applicant site. Moreover, we retain all rights to remove Submissions at any time for any reason or no reason whatsoever. Applicant reserves the right to provide information to third parties pursuant to a contractual or legal obligation.

Takedown Procedures: Applicant will comply with the terms set forth in the Uniform

Rapid Suspension (URS) procedure, Trademark Post-Delegation Dispute Procedure (PDDRP), and Registration Restriction Dispute Resolution Procedure (RRDRP). Applicant agrees to implement and adhere to any remedies imposed by decision makers under such procedures. Takedown or Suspension requests provided directly to Applicant must demonstrate the following:

- The complaint must include complainant's name, address, and email or telephone number (preferably both), and any legal counsel actively representing you in the matter, including their contact information.
- The complaint must include specific details concerning the alleged Terms violation, including but not limited to: (i) exact URL(s) where we can see the violation, (ii) for matters where URLs cannot be used (i.e., spam and/or phishing allegations), copies of files used as part of the violation and evidence as to their origins (i.e., emails including full headers), and (iii) any other supporting evidence such as screen shots and/or server log files.
- The terms violation must currently be in active and verifiable use at the time we investigate the matter.
- Applicant will suspend a registered domain on orders from a court or authority in an ICANN-approved dispute resolution procedure. The domain name will be unsuspended in view of an executive proceeding on the matter rejecting the request for suspension or upon a showing that the matter has been resolved in favor of the registrant. Appeals will be handled through the authority issuing the suspension request.

Suspension processes conducted by backend registry services provider. In the case of domain name abuse, the Applicant will determine whether to take down the subject domain name. Verisign, the Applicant's selected backend registry services provider, will follow the following auditable processes (shown in Figure 28-2) to comply with the suspension request.

Verisign Suspension Notification. The Applicant submits the suspension request to Verisign for processing, documented by:

- Threat domain name
- Registry incident number
- Incident narrative, threat analytics, screen shots to depict abuse, and/or other evidence
- Threat classification
- Threat urgency description
- Recommended timeframe for suspension/takedown
- Technical details (e.g., WHOIS records, IP addresses, hash values, anti-virus detection results/nomenclature, name servers, domain name statuses that are relevant to the suspension)
- Incident response, including surge capacity

Verisign Notification Verification. When Verisign receives a suspension request from the Applicant, it performs the following verification procedures:

- Validate that all the required data appears in the notification.
- Validate that the request for suspension is for a registered domain name.
- Return a case number for tracking purposes.

Suspension Rejection. If required data is missing from the suspension request, or the domain name is not registered, the request will be rejected and returned to the Applicant with the following information:

- Threat domain name
- Registry incident number
- Verisign case number
- Error reason

4. WHEN EXECUTED IN ACCORDANCE WITH THE REGISTRY AGREEMENT, PLANS WILL RESULT IN COMPLIANCE WITH CONTRACTUAL REQUIREMENTS

The Applicant's proposed Abuse Prevention and Mitigation Implementation Plan is and shall be consistent with the draft Registry Agreement provided by ICANN, including all Specifications, and when executed, Applicant will be compliant with the contractual requirements of the Registry Agreement, including relevant

specifications, as well as any and all emerging ICANN policies, if and when they become approved. In the event that Applicant's proposed Abuse Prevention and Mitigation Implementation Plan is not consistent with the Registry Agreement, Applicant will amend the Abuse Prevention and Mitigation Implementation Plan to result in compliance.

5. TECHNICAL PLAN SCOPE/SCALE THAT IS CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

Scope/Scale Consistency

Applicant intends to function, per the ICANN-Registry Operator Registry Agreement, as a Specification 9 exempt TLD whereby all domain name registrations in the TLD shall be registered to and maintained by Applicant and Applicant will not sell, distribute or transfer control of domain name registrations to any party that is not an Affiliate of Applicant as defined in the ICANN-Registry Operator Registry Agreement. All domain name registrations intended to be used within Applicant's registry will be registered to and controlled and maintained by Applicant and for the benefit of Applicant and its users, parents, sisters and Affiliates. Applicant does not intend to register in excess of around one thousand registrations at most. Within that context, Applicant will continue to ensure that the execution and implementation of these policies are consistent with the plan, objective and size of the registry.

Scope/Scale Consistency Specific to Backend Registry Activities

Verisign, the Applicant's selected backend registry services provider, is an experienced backend registry provider that has developed and uses proprietary system scaling models to guide the growth of its TLD supporting infrastructure. These models direct Verisign's infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. Verisign periodically updates these models to account for the adoption of more capable and cost-effective technologies.

Verisign's scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the TLD with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its scaling models, Verisign derived the necessary infrastructure required to implement and sustain this gTLD. Verisign's pricing for the backend registry services it provides to the Applicant fully accounts for cost related to this infrastructure, which is provided as "Other Operating Cost" (Template 1, Line I.L) within the Question 46 financial projections response.

29. Rights Protection Mechanisms

1. Mechanisms Designed to Prevent Abusive Registrations

Rights protection is a core objective of Applicant. Applicant will implement and adhere to any rights protection mechanisms (RPMs) that may be mandated from time to time by ICANN, including each mandatory RPM set forth in the Trademark Clearinghouse model contained in the Registry Agreement, specifically Specification 7. Applicant acknowledges that, at a minimum, ICANN requires a Sunrise period, a Trademark Claims service, and interaction with the Trademark Clearinghouse with respect to the registration of domain names for the Applicant's TLD. It should be noted that because ICANN, as of the time of this application submission, has not issued final guidance with respect to the Trademark Clearinghouse, Applicant cannot fully detail the specific implementation of the Trademark Clearinghouse within this application. Applicant will adhere to all processes and procedures to comply with ICANN guidance once this guidance is finalized.

As described in this response, Applicant will implement a Sunrise period and Trademark Claims service with respect to the registration of domain names within

the Applicant's TLD. Certain aspects of the Sunrise period and/or Trademark Claims service may be administered on behalf of Applicant by Applicant-approved registrars or by subcontractors of Applicant, such as its selected backend registry services provider, Verisign.

Applicant is committed to implementing all the rights protection mechanisms developed and approved by ICANN in addition to any other mechanisms or protections that may be necessary to effectively protect trademark holders' (and other rightsholders') rights. Indeed, one of Applicant's core objectives is the protection of the rights of both the Applicant and of third parties. To that effect, the Applicant's TLD has policies and practices which minimize abusive registration activities and other activities that affect the legal rights of others, and which further provide safeguards against unauthorized, unqualified and inappropriate registrations and ensure compliance with ICANN policies.

Applicant intends to request from ICANN an exemption from Specification 9 of the Registry Operatory Registry Agreement. As such, Applicant intents to function in such a way that all domain name registrations in the TLD shall be registered to and maintained by Applicant and Applicant will not sell, distribute or transfer control of domain name registrations to any party that is not an Affiliate of Applicant as defined in the ICANN-Registry Operator Registry Agreement. All domain name registrations intended to be used within Applicant's registry will be registered to and controlled and maintained by Applicant and for the benefit of Applicant and its users, parents, sisters and Affiliates. This will prevent fraudulent entities from obtaining a registration. As the Applicant will be the only registrant approved, there will be no risk of registration of a name by an entity which does not have such a legal name or is not commonly known by such a name. This will minimize cybersquatters and/or domain prospectors and will eliminate the possibility of abusive overreaching applications (i.e., requesting domains which do not reflect the name of the entity (legal or commonly known)).

In the event that Applicant is not granted an exemption from Specification 9, Applicant will partner with a corporate registrar with expertise in running a registry to support such efforts. Applicant intends to partner with its current corporate registrar or one of similar technical capability and expertise and allocate the appropriate funds and human resources to ensure that both itself, as the registry operator, and its selected registrar are at all times in compliance with ICANN guidelines.

At the appropriate time, between post-submission of this application and prior to the Applicant's TLD launch, Applicant will identify, determine and engage the proper service provider (e.g., Applicant-approved registrar and/or selected backend registry services provider, Verisign) to support its provision of the Sunrise period and Trademark Claims service. Any engagement for the implementation and provision of such services shall be in compliance with all ICANN-mandated regulations, agreements, guidance and policies, as it is of paramount importance of the Applicant to protect the rights of all rightsholders.

Sunrise Period. As provided by the Trademark Clearinghouse model set forth in the ICANN Applicant Guidebook, the Sunrise service pre-registration procedure for domain names continues for at least 30 days prior to the launch of the general registration of domain names in the gTLD (unless Applicant decides to offer a longer Sunrise period).

During the Sunrise period, holders of marks that have been previously validated by the Trademark Clearinghouse receive notice of domain names that are an identical match (as defined in the ICANN Applicant Guidebook) to their mark(s). Such notice is in accordance with ICANN's requirements and is provided by Applicant either directly or through Applicant-approved registrars.

Applicant requires all registrants, either directly or through Applicant-approved

registrars, to i) affirm that said registrants meet the Sunrise Eligibility Requirements (SER), and ii) submit to the Sunrise Dispute Resolution Policy (SDRP) consistent with Section 6 of the Trademark Clearinghouse model. At a minimum, Applicant recognizes and honors all word marks for which a proof of use was submitted and validated by the Trademark Clearinghouse as well as any additional eligibility requirements as specified in Question 18.

During the Sunrise period, Applicant and/or Applicant-approved registrars, as applicable, are responsible for determining whether each domain name is eligible to be registered (including in accordance with the SERs). As the Applicant will be the only registrant under Applicant's TLD, and the Applicant will comply with all policies and directives of the Trademark Clearinghouse and all other relevant rights protections mechanisms related to accepted and acknowledged rightsholders, there will be no risk of threats to the rights of third parties as third party registrations will not be permitted.

Trademark Claims Service. As provided by the Trademark Clearinghouse model set forth in the ICANN Applicant Guidebook, all new gTLDs will have to provide a Trademark Claims service for a minimum of 60 days after the launch of the general registration of domain names in the gTLD (Trademark Claims period).

During the Trademark Claims period, in accordance with ICANN's requirements, Applicant or the Applicant-approved registrar will send a Trademark Claims Notice to any prospective registrant of a domain name that is an identical match (as defined in the ICANN Applicant Guidebook) to any mark that is validated in the Trademark Clearinghouse. The Trademark Claims Notice will include links to the Trademark Claims as listed in the Trademark Clearinghouse and will be provided at no cost.

Prior to registration of said domain name, Applicant or the Applicant-approved registrar will require each prospective registrant to provide the warranties dictated in the Trademark Clearinghouse model set forth in the ICANN Applicant Guidebook. Those warranties will include receipt and understanding of the Trademark Claims Notice and confirmation that registration and use of said domain name will not infringe on the trademark rights of the mark holders listed. Without receipt of said warranties, the Applicant or the Applicant-approved registrar will not process the domain name registration.

Following the registration of a domain name, the Applicant-approved registrar will provide a notice of domain name registration to the holders of marks that have been previously validated by the Trademark Clearinghouse and are an identical match. This notice will be as dictated by ICANN. At a minimum Applicant will recognize and honor all word marks validated by the Trademark Clearinghouse.

As Applicant will be the single and only registrant under Applicant's TLD, Applicant will be the only party to whom compliance with the Trademark Clearinghouse will apply. Applicant will at all times use the Trademark Clearinghouse as a resource to determine whether its registrations are in conflict with the existing rights of third parties and, in the event of any conflict, will act in accordance with all relevant rights protection mechanisms, including, without limitation those described in Specification 7 of the ICANN-Registry Operator Registry Agreement.

2. Mechanisms Designed to Identify and address the abusive use of registered names on an ongoing basis
In addition to the Sunrise period and Trademark Claims services described in Section 1 of this response, Applicant implements and adheres to RPMs post-launch as mandated by ICANN, and confirms that registrars accredited for the Applicant's TLD are in compliance with these mechanisms. Certain aspects of these post-launch RPMs may be administered on behalf of Applicant by Applicant-approved registrars or by subcontractors of Applicant, such as its selected backend registry services

provider, Verisign.

Applicant will implement and execute all post-launch services listed in this section, all of which shall be administered on behalf of Applicant by Applicant-approved registrars or by subcontractors of Applicant, such as its selected backend registry services provider, Verisign. At the appropriate time, between post-submission of this application and prior to the Applicant's TLD launch, Applicant will identify, determine and engage the proper service provider (e.g., Applicant-approved registrar and/or selected backend registry services provider, Verisign) to support its provision of the Sunrise period and Trademark Claims service. Any engagement for the implementation and provision of such services shall be in compliance with all ICANN-mandated regulations, agreements, guidance and policies, as it is of paramount importance of the Applicant to protect the rights of all rightsholders.

These post-launch RPMs include the established Uniform Domain-Name Dispute-Resolution Policy (UDRP), as well as the newer Uniform Rapid Suspension System (URS) and Trademark Post-Delegation Dispute Resolution Procedure (PDDRP). Where applicable, Applicant will implement all determinations and decisions issued under the corresponding RPM.

After a domain name is registered, trademark holders can object to the registration through the UDRP or URS. Objections to the operation of the gTLD can be made through the PDDRP.

The following descriptions provide implementation details of each post-launch RPM for the Applicant's TLD:

- UDRP: The UDRP provides a mechanism for complainants to object to domain name registrations. The complainant files its objection with a UDRP provider and the domain name registrant has an opportunity to respond. The UDRP provider makes a decision based on the papers filed. If the complainant is successful, ownership of the domain name registration is transferred to the complainant. If the complainant is not successful, ownership of the domain name remains with the domain name registrant. Applicant and entities operating on its behalf adhere to all decisions rendered by UDRP providers.
- URS: As provided in the Applicant Guidebook, all registries are required to implement the URS. Similar to the UDRP, a complainant files its objection with a URS provider. The URS provider conducts an administrative review for compliance with filing requirements. If the complaint passes review, the URS provider notifies the registry operator and locks the domain. A lock means that the registry restricts all changes to the registration data, but the name will continue to resolve. After the domain is locked, the complaint is served to the domain name registrant, who has an opportunity to respond. If the complainant is successful, the registry operator is informed and the domain name is suspended for the balance of the registration period; the domain name will not resolve to the original website, but to an informational web page provided by the URS provider. If the complainant is not successful, the URS is terminated and full control of the domain name registration is returned to the domain name registrant. Similar to the existing UDRP, Applicant and entities operating on its behalf adhere to decisions rendered by the URS providers.
- PDDRP: As provided in the Applicant Guidebook, all registries are required to implement the PDDRP. The PDDRP provides a mechanism for a complainant to object to the registry operator's manner of operation or use of the gTLD. The complainant files its objection with a PDDRP provider, who performs a threshold review. The registry operator has the opportunity to respond and the provider issues its determination based on the papers filed, although there may be opportunity for further discovery and a hearing. Applicant participates in the PDDRP process as specified in the Applicant Guidebook.

Additional Measures Specific to Rights Protection. Applicant provides additional

measures against potentially abusive registrations, including those articulated in Applicant response to question #28 and included in its attached Abuse Prevention and Mitigation Implementation Plan. These measures help mitigate phishing, pharming, and other Internet security threats. The measures exceed the minimum requirements for RPMs defined by Specification 7 of the Registry Agreement and are available at the time of registration. All measures articulated below will be implemented to the extent and consistent with Applicant response to question #28 and included in its attached Abuse Prevention and Mitigation Implementation Plan, and include:

- Rapid Takedown or Suspension Based on Court Orders: Applicant complies promptly with any order from a court of competent jurisdiction that directs it to take any action on a domain name that is within its technical capabilities as a TLD registry. These orders may be issued when abusive content, such as child pornography, counterfeit goods, or illegal pharmaceuticals, is associated with the domain name.
- Anti-Abuse Process: Applicant implements an anti-abuse process that is executed based on the type of domain name takedown requested. The anti-abuse process is for malicious exploitation of the DNS infrastructure, such as spam, phishing, pharming, fast flux hosting, botnets, and malware.
- Authentication Procedures: Verisign, Applicant's selected backend registry services provider, uses two-factor authentication to augment security protocols for telephone, email, and chat communications.
- Malware Code Identification: This safeguard reduces opportunities for abusive behaviors that use registered domain names in the gTLD. Registrants are often unknowing victims of malware exploits. As Applicant's backend registry services provider, Verisign has developed proprietary code to help identify malware in the zones it manages, which in turn helps registrars by identifying malicious code hidden in their domain names.
- DNSSEC Signing Service: Domain Name System Security Extensions (DNSSEC) helps mitigate pharming attacks that use cache poisoning to redirect unsuspecting users to fraudulent websites or addresses. It uses public key cryptography to digitally sign DNS data when it comes into the system and then validate it at its destination. The Applicant's TLD is DNSSEC-enabled as part of Verisign's core backend registry services.

3. RESOURCING PLANS
Applicant projects it will use the following personnel roles to support the implementation of RPMs:
- 1 senior level marketing/business executive
- 1 technical manager
- 1 administrative professional

To implement and manage the Applicant's TLD as described in this application, Applicant can scale as needed, and utilize resources provided by our parent company, as defined above. In particular, personnel currently involved in the operation of Applicant's existing .com business can assist with the needs of this new TLD and may be transitioned over to supporting the TLD as the .com businesses wind down in favor of the new TLD. In addition to these individuals, our parent company will support our implementation of RPMs through the provision of their resources as well as additional outside resources on an as-needed basis. Support from our parent company will include access to a law department, finance department, information systems, technical support, human resources and such other administrative support that may be required. In particular, we anticipate using outside advisors and lawyers to assist in managing any disputes which must be resolved. Once the top level domain has been awarded, we do not anticipate disputes beyond what is frequently encountered in operating the .com. However, given the expanded opportunities associated with operating the top level domain, we have increased the likelihood of disputes, take down notices or such other matters and increased the .com dispute resolution budget. We will utilize outside advisors to provide the additional talent and resources and specialized knowledge that we

cannot cost effectively maintain internally. Projected costs associated with these resources are further discussed in the response to Question 47 below.

Resource Planning Specific to Backend Registry Activities

Verisign, Applicant's selected backend registry services provider, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services it provides to Applicant fully accounts for cost related to this infrastructure, which is provided as Line IIb.G, Total Critical Function Cash Outflows, within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign's quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign's ability to align personnel resource growth to the scale increases of Verisign's TLD service offerings.

Verisign projects it will use the following personnel roles, which are described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support the implementation of RPMs:

- Customer Affairs Organization: 9
- Customer Support Personnel: 36
- Information Security Engineers: 11

To implement and manage the Applicant's TLD as described in this application, Verisign, Applicant's selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.

When usage projections indicate a need for additional staff, Verisign's internal staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only this proposed gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

30(a). Security Policy: Summary of the security policy for the proposed registry

1 DETAILED DESCRIPTION OF PROCESSES AND SOLUTIONS DEPLOYED TO MANAGE LOGICAL SECURITY ACROSS INFRASTRUCTURE AND SYSTEMS, MONITORING AND DETECTING THREATS AND SECURITY VULNERABILITIES AND TAKING APPROPRIATE STEPS TO RESOLVE THEM

The Applicant's selected backend registry services provider's (Verisign's) comprehensive security policy has evolved over the years as part of managing some of the world's most critical TLDs. Verisign's Information Security Policy is the primary guideline that sets the baseline for all other policies, procedures, and standards that Verisign follows. This security policy addresses all of the critical components for the management of backend registry services, including architecture, engineering, and operations.

Verisign's general security policies and standards with respect to these areas are provided as follows:

- Architecture
- Information Security Architecture Standard: This standard establishes the Verisign standard for application and network architecture. The document explains the methods for segmenting application tiers, using authentication mechanisms, and implementing application functions.
- Information Security Secure Linux Standard: This standard establishes the information security requirements for all systems that run Linux throughout the Verisign organization.
- Information Security Secure Oracle Standard: This standard establishes the information security requirements for all systems that run Oracle throughout the Verisign organization.
- Information Security Remote Access Standard: This standard establishes the information security requirements for remote access to terminal services throughout the Verisign organization.
- Information Security SSH Standard: This standard establishes the information security requirements for the application of Secure Shell (SSH) on all systems throughout the Verisign organization.
- Engineering
- Secure SSL/TLS Configuration Standard: This standard establishes the information security requirements for the configuration of Secure Sockets Layer/Transport Layer Security (SSL/TLS) for all systems throughout the Verisign organization.
- Information Security C++ Standards: These standards explain how to use and implement the functions and application programming interfaces (APIs) within C++. The document also describes how to perform logging, authentication, and database connectivity.
- Information Security Java Standards: These standards explain how to use and implement the functions and APIs within Java. The document also describes how to perform logging, authentication, and database connectivity.
- Operations
- Information Security DNS Standard: This standard establishes the information security requirements for all systems that run DNS systems throughout the Verisign organization.
- Information Security Cryptographic Key Management Standard: This standard provides detailed information on both technology and processes for the use of encryption on Verisign information security systems.
- Secure Apache Standard: Verisign has a multitude of Apache web servers, which are used in both production and development environments on the Verisign intranet and on the Internet. They provide a centralized, dynamic, and extensible interface to various other systems that deliver information to the end user. Because of their exposure and the confidential nature of the data that these systems host, adequate security measures must be in place. The Secure Apache Standard establishes the information security requirements for all systems that run Apache web servers throughout the Verisign organization.
- Secure Sendmail Standard: Verisign uses sendmail servers in both the production and development environments on the Verisign intranet and on the Internet. Sendmail allows users to communicate with one another via email. The Secure Sendmail Standard establishes the information security requirements for all systems that run sendmail servers throughout the Verisign organization.

- Secure Logging Standard: This standard establishes the information security logging requirements for all systems and applications throughout the Verisign organization. Where specific standards documents have been created for operating systems or applications, the logging standards have been detailed. This document covers all technologies.
- Patch Management Standard: This standard establishes the information security patch and upgrade management requirements for all systems and applications throughout Verisign.
- General
- Secure Password Standard: Because passwords are the most popular and, in many cases, the sole mechanism for authenticating a user to a system, great care must be taken to help ensure that passwords are "strong" and secure. The Secure Password Standard details requirements for the use and implementation of passwords.
- Secure Anti-Virus Standard: Verisign must be protected continuously from computer viruses and other forms of malicious code. These threats can cause significant damage to the overall operation and security of the Verisign network. The Secure Anti-Virus Standard describes the requirements for minimizing the occurrence and impact of these incidents.

Security processes and solutions for this TLD are based on the standards defined above, each of which is derived from Verisign's experience and industry best practice. These standards comprise the framework for the overall security solution and applicable processes implemented across all products under Verisign's management. The security solution and applicable processes include, but are not limited to:

- System and network access control (e.g., monitoring, logging, and backup)
- Independent assessment and periodic independent assessment reports
- Denial of service (DoS) and distributed denial of service (DDoS) attack mitigation
- Computer and network incident response policies, plans, and processes
- Minimization of risk of unauthorized access to systems or tampering with registry data
- Intrusion detection mechanisms, threat analysis, defenses, and updates
- Auditing of network access
- Physical security

Further details of these processes and solutions are provided in Part B of this response.

1.1 Security Policy and Procedures for the Proposed Registry

Specific security policy related details, requested as the bulleted items of Question 30 - Part A, are provided here.

Independent Assessment and Periodic Independent Assessment Reports. To help ensure effective security controls are in place, the Applicant, through its selected backend registry services provider, Verisign, conducts a yearly American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) SAS 70 audit on all of its data centers, hosted systems, and applications. During these SAS 70 audits, security controls at the operational, technical, and human level are rigorously tested. These audits are conducted by a certified and accredited third party and help ensure that Verisign in-place environments meet the security criteria specified in Verisign's customer contractual agreements and are in accordance with commercially accepted security controls and practices. Verisign also performs numerous audits throughout the year to verify its security processes and activities. These audits cover many different environments and technologies and validate Verisign's capability to protect its registry and DNS resolution environments. Figure 30A 1 lists a subset of the audits that Verisign conducts. For each audit program or certification listed in Figure 30A 1, Verisign has included, as attachments to the Part B component of this response, copies of the assessment reports conducted by the listed third-party auditor. From Verisign's experience operating registries, it has determined that together these audit programs and certifications provide a reliable means to ensure effective security controls are in place and that these controls are sufficient to

meet ICANN security requirements and therefore are commensurate with the guidelines defined by ISO 27001.

Augmented Security Levels or Capabilities. See Section 5 of this response.
Commitments Made to Registrants Concerning Security Levels. See Section 4 of this response.

2 SECURITY CAPABILITIES ARE CONSISTENT WITH THE OVERALL BUSINESS APPROACH AND PLANNED SIZE OF THE REGISTRY

Verisign, the Applicant's selected backend registry services provider, is an experienced backend registry provider that has developed and uses proprietary system scaling models to guide the growth of its TLD supporting infrastructure. These models direct Verisign's infrastructure scaling to include, but not be limited to, server capacity, data storage volume, and network throughput that are aligned to projected demand and usage patterns. Verisign periodically updates these models to account for the adoption of more capable and cost-effective technologies.

Verisign's scaling models are proven predictors of needed capacity and related cost. As such, they provide the means to link the projected infrastructure needs of the TLD with necessary implementation and sustainment cost. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its scaling models, Verisign derived the necessary infrastructure required to implement and sustain this gTLD. Verisign's pricing for the backend registry services it provides to the Applicant fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

3 TECHNICAL PLAN ADEQUATELY RESOURCED IN THE PLANNED COSTS DETAILED IN THE FINANCIAL SECTION

Verisign, the Applicant's selected backend registry services provider, is an experienced backend registry provider that has developed a set of proprietary resourcing models to project the number and type of personnel resources necessary to operate a TLD. Verisign routinely adjusts these staffing models to account for new tools and process innovations. These models enable Verisign to continually right-size its staff to accommodate projected demand and meet service level agreements as well as Internet security and stability requirements. Using the projected usage volume for the most likely scenario (defined in Question 46, Template 1 - Financial Projections: Most Likely) as an input to its staffing models, Verisign derived the necessary personnel levels required for this gTLD's initial implementation and ongoing maintenance. Verisign's pricing for the backend registry services it provides to the Applicant fully accounts for cost related to this infrastructure, which is provided as "Total Critical Registry Function Cash Outflows" (Template 1, Line IIb.G) within the Question 46 financial projections response.

Verisign employs more than 1,040 individuals of which more than 775 comprise its technical work force. (Current statistics are publicly available in Verisign's quarterly filings.) Drawing from this pool of on-hand and fully committed technical resources, Verisign has maintained DNS operational accuracy and stability 100 percent of the time for more than 13 years for .com, proving Verisign's ability to align personnel resource growth to the scale increases of Verisign's TLD service offerings.

Verisign projects it will use the following personnel role, which is described in Section 5 of the response to Question 31, Technical Overview of Proposed Registry, to support its security policy:

- Information Security Engineers: 11

To implement and manage the TLD as described in this application, Verisign, the Applicant's selected backend registry services provider, scales, as needed, the size of each technical area now supporting its portfolio of TLDs. Consistent with its resource modeling, Verisign periodically reviews the level of work to be performed and adjusts staff levels for each technical area.

When usage projections indicate a need for additional staff, Verisign's internal

staffing group uses an in-place staffing process to identify qualified candidates. These candidates are then interviewed by the lead of the relevant technical area. By scaling one common team across all its TLDs instead of creating a new entity to manage only this proposed gTLD, Verisign realizes significant economies of scale and ensures its TLD best practices are followed consistently. This consistent application of best practices helps ensure the security and stability of both the Internet and this proposed gTLD, as Verisign holds all contributing staff members accountable to the same procedures that guide its execution of the Internet's largest TLDs (i.e., .com and .net). Moreover, by augmenting existing teams, Verisign affords new employees the opportunity to be mentored by existing senior staff. This mentoring minimizes start-up learning curves and helps ensure that new staff members properly execute their duties.

4 SECURITY MEASURES ARE CONSISTENT WITH ANY COMMITMENTS MADE TO REGISTRANTS REGARDING SECURITY LEVELS

Verisign is the Applicant's selected backend registry services provider. For this gTLD, no unique security measures or commitments must be made by Verisign or the Applicant to any registrant.

5 SECURITY MEASURES ARE APPROPRIATE FOR THE APPLIED-FOR gTLD STRING (FOR EXAMPLE, APPLICATIONS FOR STRINGS WITH UNIQUE TRUST IMPLICATIONS, SUCH AS FINANCIAL SERVICES-ORIENTED STRINGS, WOULD BE EXPECTED TO PROVIDE A COMMENSURATE LEVEL OF SECURITY)

No unique security measures are necessary to implement this gTLD. As defined in Section 1 of this response, Verisign, the Applicant's selected backend registry services provider, commits to providing backend registry services in accordance with the following international and relevant security standards:

- American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) SAS 70
- WebTrust/SysTrust for Certification Authorities (CA)

As defined in Section 1 of this response, Verisign, the Applicant's selected backend registry services provider, commits to providing backend registry services in accordance with the following international and relevant security standards:

- American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) SAS 70
- WebTrust/SysTrust for Certification Authorities (CA)

EXHIBIT 2

New gTLD Application Submitted to ICANN by: KBE gTLD Holding Inc

Application Downloaded On: 10 Oct 2014

String: theatre

Application ID: 1-1326-3558

Applicant Information

1. Full legal name
KBE gTLD Holding Inc

2. Address of the principal place of business
1619 Broadway
9th FLoor New York, New York - 10019 US

3. Phone number
0019174215467

4. Fax number

5. If applicable, website or URL

Primary Contact

6(a). Name
Miguel Peschiera

6(b). Title
Legal & HR Analyst

6(c). Address

6(d). Phone Number
(917) 421-5494

6(e). Fax Number

6(f). Email Address
miguel.peschiera@broadwayacrossamerica.com

Secondary Contact

7(a). Name
Sheila Lavu

7(b). Title
Associate General Council

7(c). Address

7(d). Phone Number
(917) 421-5467

7(e). Fax Number

7(f). Email Address
sheila.lavu@broadwayacrossamerica.com

Proof of Legal Establishment

8(a). Legal form of the Applicant
Corporation

8(b). State the specific national or other jurisdiction that defines the type of entity identified in 8(a).
Delaware

8(c). Attach evidence of the applicant's establishment.
Attachments are not displayed on this form.

9(a). If applying company is publicly traded, provide the exchange and symbol.

9(b). If the applying entity is a subsidiary, provide the parent company.

9(c). If the applying entity is a joint venture, list all joint venture partners.

Applicant Background

11(a). Name(s) and position(s) of all directors

Name	Position
John Gore	President and Chief Financial Officer

11(b). Name(s) and position(s) of all officers and partners

Name	Position
Elliot H. Brown	Secretary
Ilene Meiseles	Assistant Treasurer
John Gore	President and Chief Financial Officer
Paul Dietz	Vice President

11(c). Name(s) and position(s) of all shareholders holding at least 15% of shares

11(d). For an applying entity that does not have directors, officers, partners, or shareholders: Name(s) and position(s) of all individuals having legal or executive responsibility

Applied-for gTLD string

13. Provide the applied-for gTLD string. If an IDN, provide the U-label.

theatre

14A. If applying for an IDN, provide the A-label (beginning with "xn--").

14B. If an IDN, provide the meaning, or restatement of the string in English, that is, a description of the literal meaning of the string in the opinion of the applicant.

14C1. If an IDN, provide the language of the label (in English).

14C2. If an IDN, provide the language of the label (as referenced by ISO-639-1).

14D1. If an IDN, provide the script of the label (in English).

14D2. If an IDN, provide the script of the label (as referenced by ISO 15924).

14E. If an IDN, list all code points contained in the U-label according to Unicode form.

15A. If an IDN, upload IDN tables for the proposed registry. An IDN table must include:

1. the applied-for gTLD string relevant to the tables,
2. the script or language designator (as defined in BCP 47),
3. table version number,
4. effective date (DD Month YYYY), and
5. contact name, email address, and phone number.

Submission of IDN tables in a standards-based format is encouraged.

15B. Describe the process used for development of the IDN tables submitted, including consultations and sources used.

15C. List any variants to the applied-for gTLD string according to the relevant IDN tables.

---

16. Describe the applicant's efforts to ensure that there are no known operational or rendering problems concerning the applied-for gTLD string. If such issues are known, describe steps that will be taken to mitigate these issues in software and other applications.

Applicant's gTLD application is a non-IDN application. Applicant is unaware of any known operational or rendering problems related to the applied for gTLD.

---

17. OPTIONAL.
Provide a representation of the label according to the International Phonetic Alphabet (http://www.langsci.ucl.ac.uk/ipa/).

18A. Describe the mission/purpose of your proposed gTLD.

The mission of .theatre is to provide diverse internet users an enhanced online experience while enriching society with artistic and cultural diversity through high quality content, information and authentic connected experiences centered on live theatre, musicals, opera, ballet and other performing arts, Broadway, and other related concepts, topics and activities. .theatre will be a top level domain operated by KBE GTLD Holding Inc., a wholly-owned subsidiary of Key Brand Entertainment (KBE), and intends to provide internet users with the confidence that all of the programming, information, social media, shopping and/or lifestyle opportunities found on the .theatre top level domain is authentic, genuine, safe, trusted, and secure.

18B. How do you expect that your proposed gTLD will benefit registrants, Internet users, and others?

The goal of .theatre is to provide a namespace for high quality, authentic information and online experiences for individuals interested in live theatre, musicals, opera, ballet and other performing arts, Broadway, and other related concepts, topics and activities. The reputation of KBE, through its operation of broadway.com, is well recognized for high quality access to tickets, content, information and programming related to live theatre around the globe. The level of service to its customers is highly regarded as the single most trusted source for Broadway and live theatre entertainment.

Internet users will benefit because .theatre will provide an enhanced online experience through its ability to allow registrants to build more personalized experiences for internet users seeking artistic and cultural diversity. .theatre will provide Applicant greater control over the domain as a registry operator, enabling the domain to be operated with the same exceptional values KBE has shown to users through the operation of broadway.com. Additionally, new communities can be formed to connect internet users with others interested in theatre and other performing arts, Broadway and entertainment.

.theatre intends to carefully safeguard the user experience to provide users confidence that they have found a trusted site, and can be certain that users will find the high quality content,

information and experiences associated with a TLD they know and trust. New users will quickly come to recognize that .theatre stands for authentic, high quality, trusted sources for information about live theatre and other performing arts, entertainment, experiences, products and services.

18C. What operating rules will you adopt to eliminate or minimize social costs (e.g., time or financial resource costs, as well as various types of consumer vulnerabilities)? What other steps will you take to minimize negative consequences/costs imposed upon consumers?

All second level domains names used within .theatre registry will have to adhere to string guidelines limiting the TLD to verified theater-related registrants, for the benefit of the TLD.

Applicant intends to function in such a way that all domain name registrations in the TLD shall be registered to registrants who meet registration criteria. Applicant will not sell, distribute or transfer control of domain name registrations to any party that does not meet the registration criteria.

After analyzing the operation of the TLD after the initial rollout, applicant may choose to loosen its registration policies and run the TLD as an "unrestricted" TLD. In that event Applicant will partner with a corporate registrar with expertise in running a registry to support such efforts. Applicant intends to partner with its current corporate registrar or one of similar technical capability and expertise and allocate the appropriate funds and human resources to ensure that both itself, as the registry operator, and its selected registrar are at all times in compliance with ICANN guidelines.

---

19. Is the application for a community-based TLD?

No

20A. Provide the name and full description of the community that the applicant is committing to serve. In the event that this application is included in a community priority evaluation, it will be scored based on the community identified in response to this question. The name of the community does not have to be formally adopted for the application to be designated as community-based.

20B. Explain the applicant's relationship to the community identified in 20(a).

20C. Provide a description of the community-based purpose of the applied-for gTLD.

20D. Explain the relationship between the applied- for gTLD string and the community identified in 20(a).

20E. Provide a complete description of the applicant's intended registration policies in support of the community-based purpose of the applied-for gTLD. Policies and enforcement mechanisms are expected to constitute a coherent set.

20F. Attach any written endorsements for the application from established institutions representative of the community identified in 20(a). An applicant may submit written endorsements by multiple institutions, if relevant to the community.

21A. Is the application for a geographic name?

No

22. Describe proposed measures for protection of geographic names at the second and other levels in the applied-for gTLD. This should include any applicable rules and procedures for reservation and/or release of such names.

Applicant will comply with all requirements listed in the Registry Agreement in regards to reserved names - specifically 2.6 and Specification 5, which contains a list of geographic names that

must be reserved by the registry operator.

Applicant will comply with any future ICANN policy governing the reservation and/or release of such names.

Applicant is keenly aware of the sensitivity of national governments in connection with protecting country and territory identifiers in the Domain Name System (DNS).

22.1 Initial Reservation of Country and Territory Names

Applicant is committed to initially reserving the country and territory names contained in the internationally recognized lists described in Article 5 of Specification 5 of the Registry Agreement. Specifically, Applicant will reserve:

The short form (in English) of all country and territory names contained on the ISO 3166-1 list, as updated from time to time, including the European Union, which is exceptionally reserved on the ISO 3166-1 list, and its scope extended in August 1999 to any application needing to represent the name European Union, see http://www.iso.org/iso/support/country_codes/iso_3166_code_lists/iso-3166- 1_decoding_table.htm#EU;

The United Nations Group of Experts on Geographical Names Technical Reference Manual for the Standardization of Geographical Names, Part III: Names of Countries of the World; and

The list of United Nations member states in six official United Nations languages prepared by the Working Group on Country Names of the United Nations Conference on the Standardization of Geographical Names.

22.2 The Legal Protection of Geographical Identifiers

One of the more authoritative resources on the current state of the law in connection with the protection of geographical identifiers was authored by the World Intellectual Property Organization (WIPO) in its 2001 report, Second WIPO Internet Domain Name Process, The Recognition of Rights and the Use of Names in the Internet Domain Name System. Chapter Six of this report was devoted exclusively to the protection of geographical identifiers.

In analyzing the well-established framework against the misuse of geographical identifiers at the international, regional, and national levels, WIPO identified the following two elements for the protection of geographical identifiers: (i) a prohibition of false descriptions of the geographical source of goods; and (ii) a more extensive set of rules prohibiting the misuse of one class of geographical source indicators, known as geographical indications, see Second WIPO Internet Domain Name Process Report, paragraphs 206 and 210. Neither of these elements is present in Applicants's proposed use of geographical identifiers.

Notwithstanding WIPO's recommendation that the protection of geographical identifiers is "a difficult area on which views are not only divided, but also ardently held," see paragraph 237, national governments within the ICANN Governmental Advisory Committee (GAC) and other international fora have continued to advocate for increased safeguards to protect against the misuse of geographical identifiers within the DNS.

Applicant seeks to minimize any potential business practices that might mislead consumers. At the same time, however applicant believes that it is important to be able to use geographical identifiers in fair and a non-misleading manner, if such use can benefit Internet users as proposed in Applicant's business model.

As a minimum, Applicant will adopt any ICANN policy in relation to the protection of country and geographic names and acronyms.

---

23. Provide name and full description of all the Registry Services to be provided. Descriptions should include both technical and business components of each proposed service, and address any potential security or stability concerns.
The following registry services are customary services offered by a registry operator:

A. Receipt of data from registrars concerning registration of domain names and name servers.
B. Dissemination of TLD zone files.
C. Dissemination of contact or other information concerning domain name registrations (e.g., port-43 WHOIS, Web- based Whois, RESTful Whois service).
D. Internationalized Domain Names, where offered.

E. DNS Security Extensions (DNSSEC). The applicant must describe whether any of these registry services are intended to be offered in a manner unique to the TLD.

Additional proposed registry services that are unique to the registry must also be described.

Applicant has chosen CentralNic as the registry infrastructure provider for the TLD. Any information regarding technical and operational capability of the proposed the TLD registry (answers to questions 23 - 44) therefore refers to CentralNic's registry infrastructure systems. Applicant and CentralNic hereby explicitly confirm that all registry services stated below are engineered and will be provided in a manner compliant with the new gTLD Registry Agreement, ICANN consensus policies (such as Inter-Registrar Transfer Policy and AGP Limits Policy) and applicable technical standards. Except for the registry services described above, no other services will be provided by the Registry that relate to (i) receipt of data from registrars concerning registrations of domain names and name servers; (ii) provision to registrars of status information relating to the zone servers for the TLD;(iii) dissemination of TLD zone files; (iv) operation of the Registry zone servers; or (v) dissemination of contact and other information concerning domain name server registrations in the TLD as required by the Registry Agreement.
There are no other products or services, except those described above that the Registry Operator will provide (i) because of the establishment of a Consensus Policy, or (ii) by reason of Applicant being designated as the Registry Operator.
Any changes to the registry services that may be required at a later time in the course of the Applicant operating the registry will be addressed using rules and procedures established by ICANN such as the Registry Services Evaluation Policy.
Applicant proposes to operate the following registry services, utilising CentralNic's registry system:

23.1. Receipt of Data From Registrars
CentralNic will operate a Shared Registry System (SRS) for the TLD. The SRS consists of a database of registered domain names, host objects and contact objects, accessed via an Extensible Provisioning Protocol (EPP) interface, and a web based Registrar Console. Registrars will uses these interfaces to provide registration data to the registry.
The SRS will be hosted at CentralNic's primary operations centre in London, UK. The primary operations centre comprises a resilient, fault-tolerant network infrastructure with multiple high quality redundant links to backbone Internet carriers. The primary operations centre is hosted in Level 3's flagship European data centre and boasts significant physical security capabilities, including 24x7 patrols, CCTV and card-based access controls.
CentralNic's existing SRS system currently supports more than 250,000 domain names managed by over one 1,500 registrars. CentralNic has effective and efficient 24x7 customer support capabilities to support these domain names and registrars, and this capability will be expanded to meet the requirements of the TLD and provide additional capacity during periods of elevated activity (such as during Sunrise

periods).
The SRS and EPP systems are described more fully in §24 and §25. The Registrar Console is described in §31.
EPP is an extensible protocol by definition. Certain extensions have been put in place to comply with the new gTLD registry agreement, ICANN Consensus Policies and technical standards:
1. Registry Grace Period Mapping - compliant with RFC 3915
2. DNSSEC Security Extensions - compliant with RFC 5910
3. Launch Phase Extension - will be only active during the Sunrise phase, before the SRS opens for the general public. The extension is compliant with the current Internet Draft https://github.com/wil/EPP-Launch-Phase-Extension-Specification/blob/master/draft-tan-epp-launchphase.txt
More information on EPP extensions is provided in §25.
The SRS will implement and support all ICANN Consensus Policies and Temporary Policies, including:
• Uniform Domain Name Dispute Resolution Policy
• Inter-Registrar Transfer Policy
• Whois Marketing Restriction Policy
• Restored Names Accuracy Policy
• Expired Domain Deletion Policy
• AGP Limits Policy

23.2. Provision to Registrars of Status Information Relating to the Zone Servers
CentralNic will operate a communications channel to notify registrars of all operational issues and activity relating to the DNS servers which are authoritative for the TLD. This includes notifications relating to:
1. Planned and unplanned maintenance;
2. Denial-of-service attacks;
3. unplanned network outages;
4. delays in publication of DNS zone updates;
5. security incidents such as attempted or successful breaches of access controls;
6. significant changes in DNS server behaviour or features;
7. DNSSEC key rollovers.
Notifications will be sent via email (to preregistered contact addresses), with additional notifications made via an off-site maintenance site and via social media channels.

23.3. Dissemination of TLD Zone Files
CentralNic will make TLD zone files available via the Centralized Zone Data Access Provider according to specification 4, section 2 of the Registry Agreement.
Applicant will enter into an agreement with any Internet user that will allow such user to access an Internet host server or servers designated by Applicant and download zone file data. The agreement will be standardized, facilitated and administered by a Centralized Zone Data Access Provider (the "CZDA Provider"). Applicant will provide access to zone file data using the file format described in Section 2.1.4 of Specification 4 of the New gTLD Registry Agreement. Applicant, through the facilitation of the CZDA Provider, will request each user to provide it with information sufficient to correctly

identify and locate the user. Such user information will include, without limitation, company name, contact name, address, telephone number, facsimile number, email address, and the Internet host machine name and IP address.
Applicant will provide the Zone File FTP (or other Registry supported) service for an ICANN-specified and managed URL for the user to access the Registry's zone data archives. Applicant will grant the user a non-exclusive, non-transferable, limited right to access Applicant's Zone File FTP server, and to transfer a copy of the top-level domain zone files, and any associated cryptographic checksum files no more than once per 24 hour period using FTP, or other data transport and access protocols that may be prescribed by ICANN.
Applicant will provide zone files using a sub-format of the standard Master File format as originally defined in RFC 1035, Section 5, including all the records present in the actual zone used in the public DNS.
Applicant, through CZDA Provider, will provide each user with access to the zone file for a period of not less than three (3) months.
Applicant will allow users to renew their Grant of Access.
Applicant will provide, and CZDA Provider will facilitate, access to the zone file to user at no cost.

23.4. Operation of the Registry Zone Servers
The TLD zone will be served from CentralNic's authoritative DNS system. This system has operated at 100% service availability since 1996 and has been developed into a secure and stable platform for domain resolution. Partnering with Community DNS, CentralNic's DNS system includes nameservers in more than forty cities, on five continents. The DNS system fully complies with all relevant RFCs and all ICANN specifications, and has been engineered to ensure resilience and stability in the face of denial-of-service attacks, with substantial overhead and geographical dispersion.
The DNS system is described further in §35.

23.5. Dissemination of Contact and Other Information Concerning Domain Name Server Registrations
CentralNic will operate a Whois service for the TLD. The Whois service will provide information about domain names, contact objects, and name server objects stored in the Shared Registry System via a port-43 service compliant with RFC 3912. The Whois service will permit interested parties to obtain information about the Registered Name Holder, Administrative, Technical and Billing contacts for domain names. The Whois service will return records in a standardised format which complies with ICANN specifications.
CentralNic will provide access to the Whois service at no cost to the general public.
CentralNic's Whois service supports a number of features, including rate limiting to prevent abuse, privacy protections for natural persons, and a secure Searchable Whois Service. The Whois service is more fully described in §26.
Should ICANN specify alternative formats and protocols for the dissemination of Domain Name Registration Data, CentralNic will implement such alternative specifications as soon as reasonably practicable.

23.6. DNSSEC
The TLD zone will be signed by DNSSEC. CentralNic uses the award-winning signer technology from Xelerance Corporation. Zone files will be signed using NSEC3 with opt-out, following a DNSSEC Practice Statement detailed in §43.
CentralNic's DNSSEC implementation complies with RFCs 4033, 4034, 4035, 4509 and follows the best practices described in RFC 4641. Hashed Authenticated Denial of Existence (NSEC3) will be implemented, which complies with RFC 5155. The SRS will accept public-key material from child domain names in a secure manner according to industry best practices (specifically the secDNS EPP extension, described in RFC 5910). CentralNic will also publish in its website the DNSSEC Practice Statements (DPS) describing critical security controls and procedures for key material storage, access and usage for its own keys and secure acceptance of registrants' public-key material. CentralNic will publish its DPS following the format described in the "DPS-framework" Internet Draft within 180 days after that draft becomes an RFC.

23.7. Rights Protection Mechanisms
Applicant will provide all mandatory Rights Protection Mechanisms that are specified by ICANN in the Registry Agreement, the Rights protection Requirements, and the Trademark Clearinghouse, namely Trademark Claims Service, Sunrise service, Notice of Registration Periods, Claims Period, and any and all other ICANN requirements. All the required RPM-related policies and procedures such as UDRP, URS, PDDRP and RRDRP will be adopted and used in the TLD. More information is available in §29.
In addition to such RPMs, Applicant may develop and implement additional RPMs that discourage or prevent registration of domain names that violate or abuse another party's legal rights. Applicant will include all ICANN mandated and independently developed RPMs in the registry-registrar agreement entered into by ICANN-accredited registrars authorised to register names in the TLD. Applicant shall implement these mechanisms in accordance with requirements established by ICANN each of the mandatory RPMs set forth in the Trademark Clearinghouse.
The "LaunchPhase" EPP extension (described above) will be used to implement an SRS interface during the Sunrise period for the TLD. Depending on the final specification for the Trademark Claims Service (details of which have not yet been published), an additional EPP extension may be required in order to implement this service. If this is necessary, the extension will be designed to minimise its effect on the operation of the SRS and the requirements on registrars, and will only be in place for a limited period while the Trademark Claims Service is in effect for the TLD.

23.8. Registrar Support and Account Management
CentralNic will leverage its 16 years of experience of supporting over 1,500 registrars to provide high-quality 24x7 support and account management for the TLD registrars. CentralNic's experienced technical and customer support personnel will assist the TLD registrars during the on-boarding and OT&E process, and provide responsive personal support via email, phone and a web based support ticketing system.

23.9. Reporting to ICANN
Applicant and CentralNic will compile and transmit a monthly report to ICANN relating to the TLD. This report will comply with Specification 3 of the Registry Agreement.

23.10. Personnel Resources of CentralNic
The technical, operations and support functions of the registry will performed in-house by CentralNic's personnel. These personnel perform these functions on a full-time basis.

23.10.1. Technical Operations
Technical Operations refers to the deployment, maintenance, monitoring and security of the registry system, including the SRS and the other critical registry functions. Technical Operations staff design, build, deploy and maintain the technical infrastructure that supports the registry system, including power distribution, network design, access control, monitoring and logging services, and server and database administration. Internal helpdesk and incident reporting is also performed by the Technical Operations team. The Technical Operations team performs 24x7 monitoring and support for the registry system and mans the Network Operations Centre (NOC) from which all technical activities are co-ordinated.
CentralNic intends to maintain a Technical Operations team consisting of the following positions. These persons will be responsible for managing, developing and monitoring the registry system for the TLD on a 24x7 basis:
• Senior Operations Engineer(s)
• Operations Engineer(s)
• Security Engineer

23.10.2. Technical Development
The Technical Development team develops and maintains the software which implements the critical registry functions, including the EPP, Whois, Zone file generation, data escrow, reporting, backoffice and web-based management systems (intranet and extranet), and open-source registrar toolkit software. All critical registry software has been developed and maintained in-house by this team.
CentralNic intends to maintain a Technical Development team consisting of the following positions. These persons will be responsible for maintaining and developing the registry software which will support the TLD:
• Senior Technical Developer x 2
• Technical Developer x 3

23.10.3. Technical Support
Technical Support refers to 1st, 2nd and 3rd line support for registrars and end-users. Areas covered include technical support for systems and services, billing and account management. Support personnel also deal with compliance and legal issues such as UDRP and URS proceedings, abuse reports and enquiries from law enforcement.
1st line support issues are normally dealt with by these personnel. 2nd and 3rd line support issues (relating to functional or operational issues with the registry system) are escalated to Technical Operations

or Technical Development as necessary.
The Technical Support team will consist of the following positions:
• Operations Manager
• Support Manager
• Support Agent(s)
Our overseas account managers also perform basic support functions, escalating to the support agents in London where necessary.

23.10.4. Key Personnel

23.10.4.1. Gavin Brown - Chief Technology Officer
Gavin has worked at CentralNic since 2001, becoming CTO in 2005. He has overall responsibility for all aspects of the SRS, Whois, DNS and DNSSEC systems. He is a respected figure in the domain industry and has been published in several professional technical journals, and co-authored a book on the Perl programming language. He also participates in a number of technical, public policy and advocacy groups and several open source projects. Gavin has a BSc (hons) in Physics from the University of Kent.

23.10.4.2. Jenny White - Operations Manager
Jenny has been with CentralNic for nine years. Throughout this time she has expertly managed customer relations with external partners, prepared new domain launch processes and documentation, managed daily support and maintenance for over 1,500 Registrars, carried out extensive troubleshooting within the registrar environment to ensure optimum usability for registrars across communication platforms, handled domain disputes (from mediation to WIPO filing), and liaised with WIPO to implement changes to the Dispute Resolution Procedure when necessary.

23.10.4.3. Adam Armstrong - Senior Operations Engineer
Adam has recently joined CentralNic as Senior Operations Engineer. In this role he is responsible for the operation and development of the system and network infrastructure for the registry system. Adam has previously worked at a number of large UK ISPs including Jersey Telecom and Packet Exchange. He is also the lead developer of Observium, a network management system used by ICANN (amongst others). Adam has brought his strong knowledge of network design, management and security to bear at CentralNic and will oversee the operation of the SRS for the TLD.

23.10.4.4. Milos Negovanovic - Senior Technical Developer
Milos has worked at CentralNic since 2009. He has a background in building rich web applications and protocol servers. His main areas of responsibility are the Registrar Console, EPP and backoffice functions.

23.10.4.5. Mary O'Flaherty - Senior Technical Developer
Mary has worked at CentralNic since 2008. She plays an integral role in the ongoing design, development and maintenance of the registry as a whole and has specific experience with the EPP system, Registrar Console and Staff Console. Mary has a 1st class Honors degree in Computer Science from University College Cork and has previously worked for Intel and QAD Ireland.

23.10.5. Job Descriptions
CentralNic will recruit a number of new employees to perform technical duties in relation to the TLD and other gTLDs. The following job descriptions will be used to define these roles and select candidates with suitable skills and experience.

23.10.5.1. Operations Engineer
Operations Engineers assist in the maintenance and development of the network and server infrastructure of the registry system. Operations Engineers have a good knowledge of the TCP/IP protocol stack and related technologies, and are familiar with best practice in the areas of network design and management and system administration. They should be competent system administrators with a good knowledge of Unix system administration, and some knowledge of shell scripting, software development and databases. Operations Engineers have 1-2 year's relevant commercial experience. Operations Engineers report to and work with the Senior Operations Engineer, who provides advice and mentoring. Operations Engineers participate in manning the NOC on a 24x7 basis and participate in the on-call shift rota.

23.10.5.2. Security Engineer
Security Engineers enhance and assure the security of the registry system. Day-to-day responsibilities are: responding to security incidents, performing analysis and remediating vulnerabilities, conducting tests of access controls, refining system configuration to improve security, training other team members, reviewing source code, maintaining security policies and procedures, and gathering intelligence relating to threats to the registry. Security Engineers have 1-2 year's relevant commercial experience. This role reports to and works with the Senior Operations Engineer and CTO. Security Engineers participate in manning the NOC on a 24x7 basis and participate in the on-call shift rota.

23.10.5.3. Technical Developer
Technical Developers are maintain the software which supports the registry. Day-to-day responsibilities are developing new systems in response to requests from management and customers, correcting bugs in existing software, and improving its performance. Technical Developers have a good knowledge of general programming practices including use of revision control and code review systems. Developers have a good awareness of security issues, such as those described in advisories published by the oWASP Project. Developers have at least one years' commercial experience in developing applications in programming languages such as PHP, Perl, and Python, although knowledge of domain technologies such as EPP and DNS is not critical. Technical Developers work as part of a team, with advice and mentoring from the Senior Technical Developers, to whom they report.

23.10.6. Resource Matrix
To provide a means to accurately and objectively predict human resource requirements for the operation of the registry system, CentralNic has developed a Resourcing Matrix, which assigns a proportion of each employee's available time to each aspect of

registry activities. These activities include technical work such as operations and development, as well as technical support, registrar account management, rights protection, abuse prevention, and financial activity such as payroll, cash collection, etc. This matrix then permits the calculation of the total HR resource assigned to each area. A copy of the Resourcing Matrix is included as Appendix 23.2. It is important to note that the available resources cover the operation of CentralNic's entire registry operations: this includes CentralNic's own domain registry portfolio (uk.com, us.com, etc), the .LA ccTLD, as well as the gTLDs for which CentralNic will provides registry services. The actual proportion of human technical resources required specifically for the TLD is determined by the relative size of the TLD to the rest of CentralNic's operations. This calculation is based on the projected number of domains after three years of operation: the optimistic scenario is used to ensure that sufficient personnel is on hand to meet periods of enhanced demand. CentralNic has calculated that, if all its TLD clients are successful in their applications, and all meet their optimistic projections after three years, its registry system will be required to support up to 4.5 million domain names. Since the optimistic projection for the number of domains registered in the TLD after three years is a very small fraction of CentralNic's total number of domains registered the TLD will therefore require only a small fraction of CentralNic's total available HR resources in order operate fully and correctly. In the event that registration volumes exceed this figure, CentralNic will proactively increase the size of the Technical Operations, Technical Development and support teams to ensure that the needs of the TLD are fully met. Revenues from the additional registration volumes will fund the salaries of these new hires. Nevertheless, CentralNic is confident that the staffing outlined above is sufficient to meet the needs of the TLD for at least the first 18 months of operation.

---

24. Shared Registration System (SRS) Performance:
describe

- the plan for operation of a robust and reliable SRS. SRS is a critical registry function for enabling multiple registrars to provide domain name registration services in the TLD. SRS must include
  the EPP interface to the registry, as well as any other interfaces intended to be provided, if they are critical to the functioning of the registry. Please refer to the requirements in Specification 6 (section 1.2) and Specification 10 (SLA Matrix) attached to the Registry Agreement; and
  • resourcing plans for the initial implementation of, and ongoing maintenance for, this aspect of the criteria (number and description of personnel
  roles allocated to this area).
  A complete answer should include, but is not limited to:
- A high-level SRS system description;
- Representative network diagram(s);
- Number of servers;
- Description of interconnectivity with other registry systems;
- Frequency of synchronization between servers; and

- Synchronization scheme (e.g., hot standby, cold standby).

Except where specified this answer refers to the operations of the Applicant's outsource Registry Service Provider, CentralNic.

24.1. Registry Type

CentralNic operates a "thick" registry in which the registry maintains copies of all information associated with registered domains. Registrars maintain their own copies of registration information, thus registry-registrar synchronization is required to ensure that both registry and registrar have consistent views of the technical and contact information associated with registered domains. The Extensible Provisioning Protocol (EPP) adopted supports the thick registry model. See §25 for further details.

24.2. Architecture

Figure 24.1 provides a diagram of the overall configuration of the SRS. This diagram should be viewed in the context of the overall architecture of the registry system described in §32.

The SRS is hosted at CentralNic's primary operations centre in London. It is is connected to the public Internet via two upstream connections, one of which is provided by Qube. Figure 32.1 provides a diagram of the outbound network connectivity. Interconnection with upstream transit providers is via two BGP routers which connect to the firewalls which implement access controls over registry services.

Within the firewall boundary, connectivity is provided to servers by means of resilient gigabit ethernet switches implementing Spanning Tree Protocol.

The registry system implements two interfaces to the SRS: the standard EPP system (described in §25) and the Registrar Console (described in §31). These systems interact with the primary registry database (described in §33). The database is the central repository of all registry data. Other registry services also interact with this database.

An internal "Staff Console" is used by CentralNic personnel to perform management of the registry system.

24.3. EPP System Architecture

A description of the characteristics of the EPP system is provided in §25. This response describes the infrastructure which supports the EPP system.

A network diagram for the EPP system is provided in Figure 24.2. The EPP system is hosted at the primary operations centre in London. During failover conditions, the EPP system operates from the Isle of Man Disaster Recovery site (see §34).

CentralNic's EPP system has a three-layer logical and physical architecture, consisting of load balancers, a cluster of

front-end protocol servers, and a pool of application servers. Each layer can be scaled horizontally in order to meet demand.

Registars establish TLS-secured TCP connections to the load balancers on TCP port 700. Load is balanced using DNS round-robin load balancing.

The load balancers pass sessions to the EPP protocol servers. Load is distributed using a weighted-least-connections algorithm. The protocol servers run the Apache web server with the mod_epp and mod_proxy_balancer modules. These servers process session commands ("hello", "login" and "logout") and function as reverse proxies for query and transform commands, converting them into plain HTTP requests which are then distributed to the application servers. EPP commands are distributed using a weighted-least-connections algorithm.

Application servers receives EPP commands as plain HTTP requests, which are handled using application business logic. Application servers process commands and prepare responses which are sent back to the protocol servers, which return responses to clients over EPP sessions.

Each component of the system is resilient: multiple inbound connections, redundant power, high availability firewalls, load balancers and application server clusters enable seamless operation in the event of component failure. This architecture also allows for arbitrary horizontal scaling: commodity hardware is used throughout the system and can be rapidly added to the system, without disruption, to meet an unexpected growth in demand.

The EPP system will comprise of the following systems:

• 4x load balancers (1U rack mount servers with quad-core Intel processors, 16GB RAM, 40GB solid-state disk drives, running the CentOS operating system using the Linux Virtual Server [see http://www.linuxvirtualserver.org/])

• 8x EPP protocol servers (1U rack mount servers with dual-core Intel processors, 16GB RAM, running the CentOS operating system using Apache and mod_epp)

• 20x application servers (1U rack mount servers with dual-core Intel processors, 4GB of RAM, running the CentOS operating system using Apache and PHP)

24.3.1. mod_epp

mod_epp is an Apache server module which adds support for the EPP transport protocol to Apache. This permits implementation of an EPP server using the various features of Apache, including CGI scripts and other dynamic request handlers, reverse proxies, and even static files. mod_epp was originally developed by Nic.at, the Austrian ccTLD registry. Since its release, a large number of ccTLD and other registries have deployed it and continue to support its development and maintenance. Further information can be found at http://sourceforge.net/projects/aepps. CentralNic uses mod_epp to manage EPP sessions with registrar clients, and to convert EPP commands into HTTP requests which can then be handled by backend application servers.

24.3.2. mod_proxy_balancer

mod_proxy_balancer is a core Apache module. Combined with the mod_proxy module, it implements a load-balancing reverse proxy, and includes a number of load balancing algorithms and automated failover between members of a cluster. CentralNic uses mod_proxy_balancer to distribute EPP commands to backend application servers.

24.4. Performance

CentralNic performs continuous remote monitoring of its EPP system, and this monitoring includes measuring the performance of various parts of the system. As of writing, the average round-trip times (RTTs) for various functions of the EPP system were as follows:

- connect time: 87ms
- login time: 75ms
- hello time: 21ms
- check time: 123ms
- logout time: 20ms

These figures include an approximate latency of 2.4ms due to the distant between the monitoring site and the EPP system. They were recorded during normal weekday operations during the busiest time of the day (around 1300hrs UTC) and compare very favourably to the requirement of 4,000ms for session commands and 2,000ms for query commands defined in the new gTLD Service Level Agreement. RTTs for overseas registrars will be higher than this due to the greater distances involved, but will remain well within requirements.

24.5. Scaling

Horizontal scaling is preferred over vertical scaling. Horizontal scaling refers to the introduction of additional nodes into a cluster, while vertical scaling involves using more powerful equipment (more CPU cores, RAM etc) in a single system. Horizontal scaling also encourages effective mechanisms to ensure high-availability, and eliminate single points of failure in the system.

Vertical scaling leverages Moore's Law: when units are depreciated and replaced, the new equipment is likely to be significantly more powerful. If the average lifespan of a server in the system is three years, then its replacement is likely to be around four times as powerful as the old server.

For further information about Capacity Management and Scaling, please see §32.

24.6. Registrar Console

The Registrar Console is a web-based registrar account management tool. It provides a secure and easy-to-use graphical interface to the SRS. It is hosted on a virtual platform at the primary operations centre in London. As with the rest of the registry system, during a failover condition it is operated from

the Isle of Man. The virtual platform is described in Figure 24.3.

The features of the Registrar Console are described in §31.

The virtual platform is a utility platform which supports systems and services which do not operate at significant levels of load, and which therefore do not require multiple servers or the additional performance that running on "bare metal" would provide. The platform functions as a private cloud, with redundant storage and failover between hosts.

The Registrar Console currently sustains an average of 6 page requests per minute during normal operations, with peak volumes of around 8 requests per minute. Volumes during weekends are significantly lower (fewer than 1 requests per minute). Additional load resulting from this and other new gTLDs is expected to result in a trivial increase in Registrar Console request volumes, and CentralNic does not expect additional hardware resources to be required to support it.

24.7. Quality Assurance

CentralNic employs the following quality assurance (QA) methods:

1. 24x7x365 monitoring provides reports of incidents to NOC
2. Quarterly review of capacity, performance and reliability
3. Monthly reviews of uptime, latency and bandwidth consumption
4. Hardware depreciation schedules
5. Unit testing framework
6. Frequent reviews by QA working group
7. Schema validation and similar technologies to monitor compliance on a real-time, ongoing basis
8. Revision control software with online annotation and change logs
9. Bug Tracking system to which all employees have access
10. Code Review Policy in place to enforce peer review of all changes to core code prior to deployment
11. Software incorporates built-in error reporting mechanisms to detect flaws and report to Operations team
12. Four stage deployment strategy: development environment, staging for internal testing, OT&E deployment for registrar testing, then finally production deployment
13. Evidence-based project scheduling
14. Specification development and revision
15. Weekly milestones for developers
16. Gantt charts and critical path analysis for project planning

Registry system updates are performed on an ongoing basis, with any user-facing updates (ie changes to the behaviour of the EPP interface) being scheduled at specific times. Disruptive maintenance is scheduled for periods during which activity is lowest.

24.8. Billing

CentralNic operates a complex billing system for domain name registry services to ensure registry billing and collection services are feature rich, accurate, secure, and accessible to all registrars. The goal of the system is to maintain the integrity of data and create reports which are accurate, accessible, secured, and scalable. The foundation of the process is debit accounts established for each registrar. CentralNic will withdraw all domain fees from the registrar's account on a per-transaction basis. CentralNic will provide fee-incurring services (e.g., domain registrations, registrar transfers, domain renewals) to a registrar for as long as that registrar's account shows a positive balance.

Once ICANN notifies Applicant that a registrar has been issued accreditation, CentralNic will begin the registrar on-boarding process, including setting up the registrar's financial account within the SRS.

24.9. Registrar Support

CentralNic provides a multi-tier support system on a 24x7 basis with the following support levels:

• 1st Level: initial support level responsible for basic customer issues. The first job of 1st Level personnel is to gather the customer's information and to determine the customer's issue by analyzing the symptoms and figuring out the underlying problem.

• 2nd Level: more in-depth technical support level than 1st Level support containing experienced and more knowledgeable personnel on a particular product or service. Technicians at this level are responsible for assisting 1st Level personnel solve basic technical problems and for investigating elevated issues by confirming the validity of the problem and seeking for known solutions related to these more complex issues.

• 3rd Level: the highest level of support in a three-tiered technical support model responsible for handling the most difficult or advanced problems. Level 3 personnel are experts in their fields and are responsible for not only assisting both 1st and 2nd level personnel, but with the research and development of solutions to new or unknown issues.

CentralNic provides a support ticketing system for tracking routine support issues. This is a web based system (available via the Registrar Console) allowing registrars to report new issues, follow up on previously raised tickets, and read responses from CentralNic support personnel.

When a new trouble ticket is submitted, it is assigned a unique ID and priority. The following priority levels are used:

1. Normal: general enquiry, usage question, or feature enhancement request. Handled by 1st level support.

2. Elevated: issue with a non-critical feature for which a work-around may or may not exist. Handled by 1st level support.

3. Severe: serious issue with a primary feature necessary for daily operations for which no work-around has been discovered and which completely prevents the feature from being used. Handled by 2nd level support.

4. Critical: A major production system is down or severely impacted. These issues are catastrophic outages that affect the overall Registry System operations. Handled by 3rd level support.

Depending on priority, different personnel will be alerted to the existence of the ticket. For example, a Priority 1 ticket will cause a notification to be emailed to the registrar customer support team, but a Priority 4 ticket will result in a broadcast message sent to the pagers of senior operations staff including the CTO. The system permits escalation of issues that are not resolved within target resolution times.

24.10. Enforcement of Eligibility Requirements

The SRS supports enforcement of eligibility requirements, as required by specific TLD policies.

Figure 24.4 describes the process by which registration requests are validated. Prior to registration, the registrant's eligibility is validated by a Validation Agent. The registrant then instructs their registrar to register the domain. The SRS returns an "Object Pending" result code (1001) to the registrar.

The request is sent to the Validation Agent by the registry. The Validation Agent either approves or rejects the request, having reconciled the registration information with that recorded during the eligibility validation. If the request has been approved, the domain is fully registered. If it is rejected, the domain is immediately removed from the database. A message is sent to the registrar via the EPP message queue in either case. The registrar then notifies the registrant of the result.

24.11. Interconnectivity With Other Registry Systems

The registry system is based on multiple resilient stateless modules. The SRS, Whois, DNS and other systems do not directly interact with each other. Interactions are mediated by the database which is the single authoritative source of data for the registry as a whole. Individuals modules perform "CRUD" (create, read, update, delete) actions upon the database. These actions then affect the behaviour of other registry systems: for example, when a registrar adds the "clientHold" status to a domain object, this is recorded in the database. When a query is received for this domain via the Whois service, the presence of this status code in the database results in the "Status: CLIENT HOLD" appearing in the whois record. It will also be noted by the zone generation system, resulting in the temporary removal of the delegation of the domain name from the DNS.

24.12. Resilience

The SRS has a stateless architecture designed to be fully resilient in order to provide an uninterrupted service in the face of failure or one or more parts of the system. This is achieved by use of redundant hardware and network connections, and by use of continuous "heartbeat" monitoring allowing dynamic and high-speed failover from active to standby components, or between nodes in an

active-active cluster. These technologies also permit rapid scaling of the system to meet short-term increases in demand during "surge" periods, such as during the initial launch of a new TLD.

24.12.1. Synchronisation Between Servers and Sites

CentralNic's system is implemented as multiple stateless systems which interact via a central registry database. As a result, there are only a few situations where synchronisation of data between servers is necessary:

1. replication of data between active and standby servers (see §33). CentralNic implements redundancy in its database system by means of an active/standby database cluster. The database system used by CentralNic supports native real-time replication of data allowing operation of a reliable hot standby server. Automated heartbeat monitoring and failover is implemented to ensure continued access to the database following a failure of the primary database system.

2. replication is used to synchronise the primary operations centre with the Disaster Recovery site hosted in the Isle of Man (see §34). Database updates are replicated to the DR site in real-time via a secured VPN, providing a "hot" backup site which can be used to provide registry services in the event of a failure at the primary site.

24.13. Operational Testing and Evaluation (OT&E)

An Operational Testing and Evaluation (OT&E) environment is provided for registrars to develop and test their systems. The OT&E system replicates the SRS in a clean-room environment. Access to the OT&E system is unrestricted and unlimited: registrars can freely create multiple OT&E accounts via the Registrar Console.

24.14. Resourcing

As can be seen in the Resourcing Matrix found in Appendix 23.2, CentralNic will maintain a team of full-time developers and engineers which will contribute to the development and maintenance of this aspect of the registry system. These developers and engineers will not work on specific subsystems full-time, but a certain percentage of their time will be dedicated to each area. The total HR resource dedicated to this area is equivalent to more than one full-time post.

CentralNic operates a shared registry environment where multiple registry zones (such as CentralNic's domains, the .LA ccTLD, this TLD and other gTLDs) share a common infrastructure and resources. Since the TLD will be operated in an identical manner to these other registries, and on the same infrastructure, then the TLD will benefit from an economy of scale with regards to access to CentralNic's resources.

CentralNic's resourcing model assumes that the "dedicated" resourcing required for the TLD (ie, that required to deal with issues related specifically to the TLD and not to general issues with the system as a whole) will be equal to the proportion of the

overall registry system that the TLD will use. CentralNic has calculated that, if all its TLD clients are successful in their applications, and all meet their optimistic projections after three years, its registry system will be required to support up to 4.5 million domain names. Therefore the TLD will require [0.22]% of the total resources available for this area of the registry system.

In the event that registration volumes exceed this figure, CentralNic will proactively increase the size of the Technical Operations, Technical Development and support teams to ensure that the needs of the TLD are fully met. Revenues from the additional registration volumes will fund the salaries of these new hires. Nevertheless, CentralNic is confident that the staffing outlined above is sufficient to meet the needs of the TLD for at least the first 18 months of operation.

---

25. Extensible Provisioning Protocol (EPP): provide a detailed description of the interface with registrars, including how the applicant will comply with EPP in RFCs 3735 (if applicable), and 5730-5734.
If intending to provide proprietary EPP extensions, provide documentation consistent with RFC 3735, including the EPP templates and schemas that will be used.
Describe resourcing plans (number and description of personnel roles allocated to this area).
A complete answer is expected to be no more than 5 pages. If there are proprietary EPP extensions, a complete answer is also expected to be no more than 5 pages per EPP extension.

Except where specified this answer refers to the operations of the Applicant's outsource Registry Service Provider, CentralNic.

The Extensible Provisioning Protocol (EPP) is an application layer client-server protocol for the provisioning and management of objects stored in a shared central repository. EPP defines generic object management operations and an extensible framework that maps protocol operations to objects. EPP has become established as the common protocol by which domain registrars can manage domains, nameservers and contact details held by domain registries. It is widely deployed in the gTLD and ccTLD registry space.
CentralNic has operated its EPP system since 2005, and it currently operates at significant load in terms of registrars, sessions and transaction volumes. CentralNic's EPP system is fully compliant with the following RFC specifications:

- 5730 - Base Protocol
- 5731 - domains
- 5732 - Host Objects
- 5733 - Contact Objects
- 5734 - TCP Transport
- 3735 - Extension Guidelines
- 3915 - RGP Extension
- 5910 - DNSSEC Extension

25.1. Description of Interface
EPP is a stateful XML protocol layered over TCP (see RFC 3734). Protected

using lower-layer security protocols, clients exchange identification, authentication, and option information, and engage in a series of client-initiated command-response exchanges. All EPP commands are atomic (there is no partial success or partial failure) and designed so that they can be made idempotent (executing a command more than once has the same net effect on system state as successfully executing the command once).
EPP provides four basic service elements: service discovery, commands, responses, and an extension framework that supports definition of managed objects and the relationship of protocol requests and responses to those objects.
EPP servers respond to client-initiated communication (which can be either a lower-layer connection request or an EPP service discovery message) by returning a greeting to a client. The server then responds to each EPP command with a coordinated response that describes the results of processing the command.
EPP commands fall into three categories: session management, queries, and transform commands. Session management commands are used to establish and end persistent sessions with an EPP server. Query commands perform read-only object information retrieval operations. Transform commands perform read-write object management operations.
Commands are processed by a server in the order they are received from a client. The protocol includes features that allow for offline review of transform commands before the requested action is completed. In such situations, the response clearly notes that the command has been received but that the requested action is pending. The corresponding object then reflects processing of the pending action. The server will also notify the client when offline processing of the action has been completed.
Object mappings describe standard formats for notices that describe completion of offline processing.
EPP uses XML namespaces to provide an extensible object management framework and to identify schemas required for XML instance parsing and validation. These namespaces and schema definitions are used to identify both the base protocol schema and the schemas for managed objects.

25.1.1. Objects supported
Registrars may create and manage the following object types in the CentralNic EPP system:
• domains (RFC 5731)
• host objects (RFC 5732)
• contact objects (RFC 5733)

25.1.2. Commands supported
CentralNic supports the following EPP commands:
• "hello" - retrieve the "greeting" from the server
• "login" and "logout" - session management
• "poll" - message queue management
• "check" - availability check
• "info" - object information
• "create" - create object
• "update" - update object
• "renew" - renew object
• "delete" - delete object
• "transfer" - manage object transfer

25.2. EPP state diagram
Figure 25.1 describes the state machine for the EPP system. Clients

establish a connection with the server, which sends a greeting. Clients then authenticate, and once a login session is established, submits commands and receive responses until the server closes the connection, the client sends a logout command, or a timeout is reached.

25.3. EPP Object Policies
The following policies apply to objects provisioned via the EPP system:

25.3.1. domains
1. domains must comply with the syntax described in RFC 1035 §2.3.1. Additionally, the first label of the name must be between 3 and 63 characters in length.
2. domains must have a registrant attribute which is associated with a contact object in the database.
3. domains must have an administrative contact attribute which is associated with a contact object in the database.
4. domains must have a technical contact which attribute is associated with a contact object in the database.
5. domains may have an billing contact attribute which is associated with a contact object in the database.
6. domains may have between 0 (zero) and 13 DNS servers. A domain with no name servers will not resolve and no records will be published in the DNS
7. the host object model for domains is used rather than the host attribute model.
8. domains may have a number of status codes. The presence of certain status codes indicates the domain's position in the lifecycle, described further in §27.
9. where policy requires, the server may respond to a "domain:create" command with an "Object Pending" (1001) response. When this occurs, the domain is placed onto the pendingCreate status while an out-of-band validation process takes place.
10. when registered, the expiry date of a domain may be set up to ten years from the initial date of registration. Registrars can specify registration periods in one-year increments from one to ten.
11. when renewed, the expiry date of a domain may be set up to ten years from the current expiry date. Registrars can specify renewal periods in one-year increments from one to ten. domains which auto-renew are renewed for one year at a time.
12. domains must have an authInfo code which is used to authenticate inter-registrar transfer requests. This authInfo code may contain up to 48 bytes of UTF-8 character data.
13. domains may have one or more DS records associated with them. DS records are managed via the secDNS EPP extension, as specified in RFC 5910.
14. only the sponsoring registrar of the domain may submit "update", "renew" or "delete" commands for the domain.

25.3.2. Host objects
1. host names must comply with RFC 1035. The maximum length of the host name may not exceed 255 characters.
2. in-bailiwick hosts must have an IPv4 address. They may optionally have an IPv6 address.
3. multiple IP addresses are not currently permitted.
4. sponsorship of hosts is determined as follows: if an object is in-bailwick (ie child of a domain in the database, and therefore also child to a TLD in the system), then the sponsor is the sponsor of the parent

domain. If the object is out-of-bailiwick, the sponsor is the registrar which created the contact.
5. if a registrar submits a change to the name of a host object, if the new host name is subordinate to an in-bailiwick domain, then that registrar must be the sponsor of the new parent domain.
6. registrars are not permitted to create hosts that are subordinate to a non-existent in-bailiwick domain, or to change the name of a host object so that it us subordinate to a non-existent in-bailiwick domain.
7. a host cannot be deleted if one or more domains are delegated to it (the registry deletes hosts to remove orphan glue, see §28).
8. inter-registrar transfers are not permitted.
9. only the sponsoring registrar of the host may submit "update" or "delete" commands for the object.

25.3.3. Contact objects
1. contact IDs may only contain characters from the set [A-Z, 0-9, . (period), - (hyphen) and - (underscore)] and are case-insensitive.
2. phone numbers and email addresses must be valid as described in RFC 5733 §2.5 and §2.6.
3. contact information is accepted and stored in "internationalized" format only: that is, contact objects only have a single "contact:postalInfo" element and the type attribute is always "int".
4. the "contact:org", "contact:sp", "contact:pc", "contact:phone" and "contact:fax" elements are optional.
5. contacts must have an authInfo code which is used in inter-registrar transfers. This code may contain up to 48 bytes of UTF-8 character data.
6. a contact cannot be deleted if one or more domains are associated with it.
7. only the sponsoring registrar of the contact may submit "update" or "delete" commands for the object.

25.4. EPP Extensions
CentralNic supports the following EPP extensions. CentralNic's implementations fully comply with the required specifications.

25.4.1. Registry Grace Period Mapping
Various grace periods and hold periods are supported by the Registry Grace Period mapping, as defined in RFC 3915. This is described further in §27.

25.4.2. DNSSEC Security Extensions Mapping
Registrars may submit Delegation Signer (DS) record information for domains under their sponsorship. This permits the establishment of a secure chain-of-trust for DNSSEC validation.
CentralNic supports the specification defined in RFC 5910. This supports two interfaces: the DS Data Interface and Key Data Interface. CentralNic supports the former interface (DS Data), where registrars submit the keytag, algorithm, digest type and digest for DS records as XML elements, rather than as key data. Key data is stored if provided as a child element of the "secDNS:dsData" element. The maxSigLife element is optional in the specification and is not currently supported.

25.4.3. Launch Phase Extension
CentralNic has assisted development of a standard EPP extension for registry "launch phases" (ie Sunrise and Landrush periods), during which the steady-state mode of "first-come, first-served" operation does not

apply. This extension permits registrars to submit requests for domains with claimed rights such as a registered trademark. The extension is currently described in an Internet-Draft (see http://tools.ietf.org/html/draft-tan-epp-launchphase-00). It is hoped that this draft will eventually be published as an RFC which can be implemented by other registries and registrars.
CentralNic's system implements this extension and will support the most recent version of the draft during the initial launch of the TLD. Once the TLD enters General Availability, this extension will no longer be available for use by registrars. Example frames describing the use of this extension are included in Appendix 25.2. As of writing, the current draft does not include a full schema definition, but a schema from a previous version has been included in Appendix 25.3. When the Draft is updated to include a schema, it will be based on this version.

25.5. Registrar Credentials and Access Control
Registrars are issued with a username (their registrar ID) and a password. This password cannot be used to access any other service and only this password can be used to access the EPP system. Registrar officers with the "Management" access level can change their EPP password via the Registrar Console.
RFC 5730 requires "mutual, strong client-server authentication". CentralNic requires that all registrars connect using an SSL certificate. This certificate may be obtained from a recognised certificate authority, or it may be a self-signed certificate registered with CentralNic via the Registrar Console. Registrar officers with the "Management" access level can upload SSL certificates for their account.

25.6. Session Limits and Transaction Volumes
There are no limits on the number of active sessions a registrar can maintain with the server. Similarly, there are no limits on the volume of transactions a registrar may send. However the system is fully capable of imposing connection limits and this measure may be used in future to ensure equal access amongst registrars.

25.7. Transaction Logging and Reporting
All "transform" commands are logged. Transform commands are: "create", "renew", "update", "delete" and "transfer". The system logs the time and date when the command was received, the registrar which submitted it, the request and response frames, the result code and message. All commands, whether successful or not, are logged.
The transaction log is stored in the primary registry database. Registrars have access to the log for their account via the Registrar Console. The log viewer permits filtering by command, object type, object ID (domain, host name, contact ID), result code and timestamp.
Query commands ("check", "info", "poll op="req") and session commands ("login", "logout" and "hello") are not logged due to the large volume of such queries (particularly "check" queries). The EPP system uses counters for these commands to facilitate generation of monthly reports.

25.8. EPP Message Queue
The EPP protocol provides a message queue to provide registrars with notifications for out-of-band events. CentralNic currently supports the following EPP message notifications:
- approved inbound transfer
- rejected inbound transfer

• new outbound transfer
• cancelled outbound transfer
• approved or rejected domain registration request (where TLD policy requires out-of-band approval of "domain:create" requests)

25.9. Registrar Support, Software Toolkit
CentralNic has supported EPP for many years. CentralNic has released a number of open source client libraries for several popular programming languages. These are used by registrars and registries around the world. CentralNic maintains the following open source EPP libraries:
• Net::EPP, a general purpose EPP library for Perl. See http://code.google.com/p/perl-net-epp/
• Preppi, a graphical EPP client written in Perl. See https://www.centralnic.com/company/labs/preppi
• Net_EPP, a PHP client class for EPP. See https://github.com/centralnic/php-epp
• Simpleepp, a Python client class for EPP. See https://bitbucket.org/milosn/simpleepp
• tx-epp-proxy, a EPP reverse proxy for shared-nothing client architectures written in Python. See https://bitbucket.org/milosn/tx-epp-proxy
These libraries are available for anyone to use, at no cost. CentralNic develops these libraries, and accepts submissions and bug reports from users around the world.

25.10. Quality Assurance, RFC Compliance
To ensure that its EPP system fully complies with the relevant specifications documents, CentralNic has implemented the following:

25.10.1. Schema Validation
The EPP system automatically validates all response frames against the XSD schema definitions provided in the RFCs. Should a non-validating response be sent to a registrar, an alert is raised with the NOC to be investigated and corrected. By default, this feature is disabled in the production environment but it is enabled in all other environments (as described below).

25.10.2. Multi-stage Deployment and Testing
EPP system code is developed, tested and deployed in a multi-stage environment:
1. Developers maintain their own development environment in which new code is written and changes are prepared. Development environments are configured with the highest level of debugging and strictness to provide early detection of faults.
2. All changes to the EPP system are subjected to peer review: other developers in the team must review, test and sign off the changes before being committed (or, if developed on a branch, being merged into the stable branch).
3. Changes to EPP system code are then deployed in the OT&E environment. Registrars continually test this system as part of their own QA processes, and this additional phase provides an additional level of quality assurance.

25.10.3. Registrar Feedback
Registrars are provided with an easy way to report issues with the EPP system, and many perform schema validation on the responses they receive.

When issues are detected by registrars, they are encouraged to submit bug reports so that developers can rectify the issues.

25.11. EPP System Resourcing
As can be seen in the Resourcing Matrix found in Appendix 23.2, CentralNic will maintain a team of full-time developers and engineers which will contribute to the development and maintenance of this aspect of the registry system. These developers and engineers will not work on specific subsystems full-time, but a certain percentage of their time will be dedicated to each area. The total HR resource dedicated to this area is equivalent to more than one full-time person.
CentralNic operates a shared registry environment where multiple registry zones (such as CentralNic's domains, the .LA ccTLD, this TLD and other gTLDs) share a common infrastructure and resources. Since the TLD will be operated in an identical manner to these other registries, and on the same infrastructure, then the TLD will benefit from an economy of scale with regards to access to CentralNic's resources.
CentralNic's resourcing model assumes that the "dedicated" resourcing required for the TLD (ie, that required to deal with issues related specifically to the TLD and not to general issues with the system as a whole) will be equal to the proportion of the overall registry system that the TLD will use. CentralNic has calculated that, if all its TLD clients are successful in their applications, and all meet their optimistic projections after three years, its registry system will be required to support up to 4.5 million domain names. Therefore the TLD will require [0.22]% of the total resources available for this area of the registry system.
In the event that registration volumes exceed this figure, CentralNic will proactively increase the size of the Technical Operations, Technical Development and support teams to ensure that the needs of the TLD are fully met. Revenues from the additional registration volumes will fund the salaries of these new hires. Nevertheless, CentralNic is confident that the staffing outlined above is sufficient to meet the needs of the TLD for at least the first 18 months of operation.

---

26. Whois: describe

- how the applicant will comply with Whois specifications for data objects, bulk access, and lookups as defined in Specifications 4 and 10 to the Registry Agreement;
- how the Applicant's Whois service will comply with RFC 3912; and
- resourcing plans for the initial implementation of, and ongoing maintenance for, this aspect of the criteria (number and description of personnel roles allocated to this area).

A complete answer should include, but is not limited to:

- A high-level Whois system description;
- Relevant network diagram(s);
- IT and infrastructure resources (e.g., servers, switches, routers and other components);
- Description of interconnectivity with other registry systems; and

Frequency of synchronization between servers.
To be eligible for a score of 2, answers must also include:

- Provision for Searchable Whois capabilities; and
- A description of potential forms of abuse of this feature, how these risks will be mitigated, and the basis for these descriptions

A complete answer is expected to be no more than 5 pages.

Except where specified this answer refers to the operations of the Applicant's outsource Registry Service Provider, CentralNic.

Whois is one of the oldest Internet protocols still in use. It allows interested persons to retrieve information relating to Internet resources (domain names and IP addresses). Whois services are operated by the registries of these resources, namely TLD registries and RIRs.
Whois is described by RFC 3912, which serves as a description of existing systems rather than requiring specific behaviours from clients and servers. The protocol is a query-response protocol, in which both the query and the response are opaque to the protocol, and their meanings are known only the server and to the human user who submits a query. Whois has a number of limitations, but remains ubiquitous as a means for obtaining information about name and number resources.

26.1. Compliance
The Whois service for the TLD will comply with RFC3912 and Specifications 4 and 10 of the Registry Agreement. The service will be provided to the general public at no cost. If ICANN specify alternative formats and protocols (such as WEIRDS) then CentralNic will implement these as soon as reasonably practicable.
CentralNic will monitor its Whois system to confirm compliance. Monitoring stations will check the behaviour and response of the Whois service to ensure the correctness of Whois records. CentralNic will maintain a public Whois contact to which bug reports and other questions about the Whois service can be directed. The Whois service will additionally comply with all requisite data protection laws (with regards to the collection and retention of personal data), including all relevant European Union privacy directives.

26.2. Domain Name
By default, any query is assumed to be a domain name unless a keyword is prepended to the query. If the domain exists, then registration is returned, including the following fields:
- Domain ROID
- Domain Name
- Domain U-label (if IDN)
- Creation Date
- Last Updated
- Expiration Date
- EPP status codes
- Registrant Contact Information
- Administrative Contact Information
- Technical Contact Information
- Billing Contact Information (if any)
- Sponsoring Registrar ID
- Sponsoring Registrar Contact Information
- DNS servers (if any)
- DNSSEC records (if any)

An example of a domain whois response is included in Appendix 26.1. The Domain ROID is the Repository Object Identifier as described in RFC 5730, §2.8. The ROID field corresponds to the "domain:roid" element of EPP "info" responses.
A domain may be associated with one or more status codes. These are represented in Whois responses as phrases rather than EPP mnemonics. A domain may have any of the following status codes:
• PENDING CREATE - a "domain:create" command has been received through the SRS, but the registration has not yet been finalised as an out-of-band review process has not yet been completed.
• ADD PERIOD - the domain is in the Add Grace Period
• CLIENT HOLD - the registrar has added the clientHold status
• DELETE PROHIBITED - this may be present if the domain has either clientDeleteProhibited or serverDeleteProhibited (or both)
• INACTIVE - the domain has no DNS servers
• PENDING DELETE - the domain has left the Redemption Grace Period and is scheduled for deletion
• PENDING DELETE RESTORABLE - the domain is in the Redemption Grace Period
• PENDING RESTORE - a restore request has been received, but the Restore Report has not been received
• PENDING TRANSFER - there is an active inter-registrar transfer for the domain
• RENEW PERIOD - the domain is either in the Renew Grace Period or the Auto-Renew Grace Period
• RENEW PROHIBITED - this may be present if the domain has either clientRenewProhibited or serverRenewProhibited (or both)
• SERVER HOLD - the registry has added the serverHold status
• TRANSFER PERIOD - the domain is in the Transfer Grace Period
• TRANSFER PROHIBITED - this may be present if the domain has either clientTransferProhibited or serverTransferProhibited (or both)
• UPDATE PROHIBITED - this may be present if the domain has either clientUpdateProhibited or serverUpdateProhibited (or both)
• OK - present if none of the above apply.
The Registrant, Administrative, Technical and Billing Contact sections of the Whois record display the contact information for the contact objects that are associated with the domain. The information displayed replicates the information showed for a contact query (see below). The server shows similar information for the sponsoring registrar.
Domains may have 0-13 DNS servers. If a domain name has no DNS servers, then the "INACTIVE" status code appears in the Status section. If the registrant provided DS records for their DNSSEC-signed domain, then these are included. For each DS record, then the key tag, algorithm, digest type and digest are displayed.

26.3. Contact
Users can query for information about a contact by submitting a query of the form "contact [ID]", where "[ID]" is the contact ID equivalent to the "contact:id" element in EPP "info" responses. This is also the ID used when referring to contacts in domain responses.
The following information is included in Dontact records:
• Contact ID
• Sponsoring Registrar
• Creation Date
• Last Updated Date
• EPP Status Codes
• Contact Name

- Organisation
- Street Address (1-3 fields)
- City
- State/Province
- Postcode
- Country Code (2 character ISO-3166 code)
- Phone number (e164a format)
- Fax number (e164a format)
- Email address

An example of a contact object whois response is included in Appendix 26.2. A contact object may be associated with one or more status codes. These are represented in Whois responses as phrases rather than EPP code mnemonics. A contact object may have any of the following status codes:

- DELETE PROHIBITED - present if the contact object has either clientDeleteProhibited or serverDeleteProhibited (or both)
- TRANSFER PROHIBITED - present if the contact object has either clientTransferProhibited or serverTransferProhibited (or both)
- UPDATE PROHIBITED - present if the contact object has either clientUpdateProhibited or serverUpdateProhibited (or both)
- PENDING TRANSFER - there is an active inter-registrar transfer for the contact object
- LINKED - the contact object is associated with one or more domain names. A LINKED contact object automatically has the DELETE PROHIBITED status

26.4. Host Objects

Users can query for information about a host object by submitting a query of the form "nameserver [HOST]". The following information is included in host records:

- Server Name
- IPv4 address (if any)
- IPv6 address (if any)
- EPP status codes
- Sponsoring Registrar
- Creation Date
- Referral URL (if any)

An example of a host whois response is included in Appendix 26.3. A host object may have an IPv4 or IPv6 address if the host is "in-bailiwick", ie subordinate to a domain name within a TLD operated by the registry. IP address information is not shown for "out-of-bailiwick" hosts.

Host objects may only have two status codes:

- INACTIVE - the host is not associated with any domain names
- LINKED - the host is associated with one or more domain names

The Referral URL is the website of the Sponsoring Registrar for this host. If the host is subordinate to a domain name in the TLD, this will be the sponsoring registrar of the parent name. If the host is out-of-bailiwick, then the sponsoring registrar is the registrar who issued the original "create" request.

26.5. Character Encoding

Responses are encoded as UTF-8. Queries are assumed to be encoded in UTF-8.

26.6. IDN Support

The Whois service supports Internationalised Domain Names. Users may submit queries for IDN domains using either the U-label or the A-label.